Learn NIST 800-53 & 800-53a, ISO27001 & 27002, GDPR, CMMC (NIST 800-171), and NIST CSF. These are biggest frameworks/regulations you’ll come across. When it comes to NIST documents the “a” in it is the assessment portion. So, for example the “how to” assess NIST 800-53 is found in the -53a document. For ISO27001, the how to assess is found in 27002. I’d be happy to dive into more detail on them with you after the break.

Optional Chapter (ESVF):

- Static application security testing (SAST): evaluates the security of software without running it by analyzing either the source code or the compiled application. Usually, it uses automated tools to detect common software flaws like buffer overflows. In mature development environments, application developers are given access to static analysis tools and use them throughout the design, build, and test process.

- Dynamic application security testing (DAST): evaluates the security of software in a runtime environment, often the only option for organizations deploying applications written by someone else. A common example is the use of web application scanning tools (detecting CSRF, SQL injection and so on). It may include the use of synthetic transactions (scripted transactions with known expected results) to verify system performance.

- Additionally, interactive application security testing (IAST) performs real-time analysis of runtime behavior, application performance, HTTP/HTTPS traffic, frameworks, components, and backend connections.

Some remediations are:

- Input Validation: make sure the inputs are processed as intended

- Web Application Firewalls (WAFs): function similarly to network firewalls, but they work at the Application layer of the OSI model.

- Database Security: parameterized queries and stored procedures & Obfuscation and Camouflage (data minimization, tokenization, and hashing)

- Code Security: code signing (digitally, confirming the authenticity of developers’ code to the end users), code reuse (making a third-party software libraries and software development kits (SDKs) for reuse), software diversity (to avoid single points of failure), code repositories (centralized locations for the storage and management of application source code, for secure storage, for the coordination of changes among multiple developers, for performing version control, for code reuse, and for avoiding the problem of dead code (where nobody is responsible for the maintenance)), and integrity measurement

- Application Resilience: Scalability and Elasticity

- Secure Coding Practices: be careful with source code comments, error handling, and hard-coded credentials (backdoor vulnerability) as well as memory management (resource exhaustion and pointer dereferencing)

- Web application vulnerabilities are mostly associated with XSS (reflected XSS, stored XSS, request forgery, CSRF, SSRF) and session hijacking. Besides, there are other vulnerabilities like direct object references, directory traversal, and file inclusion (local file inclusion and remote file inclusion).

I would address session hijacking as the 1st area (can be remediated by enforcing TLS everywhere, set Secure+HttpOnly+SameSite=Strict cookies, invalidate old sessions on login, throttle failed logins), input validation & injection flaws (can be remediated with parameterized queries for database security) as the 2nd area, and authorization & access control as the 3rd area (can be remediated with centralize authorization logic (don’t mix it into views)).

I performed a pentest project where it includes all of this (here's an example: https://github.com/zedttxj/Web-Security-Exploits/tree/main/Example-1).

Chapter 1

1. Alignment of Security Function to Business Strategy, Goals, Missions, and Objectives
   1. Strategic Plan: is a long-term plan that is fairly stable. It defines the organization’s security purpose. It defines the security function and aligns it to the goals, mission, and objectives of the organization. It’s useful for about five years, if it’s maintained and updated annually. The strategic plan also serves as the planning horizon. Long-term goals and visions for the future are discussed in a strategic plan. A strategic plan should include a risk assessment.
   2. Tactical Plan: the tacitical plan is a midterm plan developed to provide more details on accomplishing the goals set forth in the strategic plan, or can be crafted ad hoc based on unpredicted events. A tactical plan is typically useful for about a year and often prescribes and schedules the tasks necessary to accomplish organizational goals. Some examples of tactical plans are project plans, acquisition plans, hiring plans, budget plans, maintenance plans, support plans, and system development plans
   3. Operational Plan: is a short-term, highly detailed plan based on the strategic and tactical plans. It’s valid or useful only for a short time. Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans. Operational plans spell out how to accomplish the various goals of the organization. They include resource allotments, budgetary requirements, staffing assignments, scheduling, and step-by-step or implementation procedures. Operational plans include details on how the implementation processes are in compliance with the organization’s security policy. Examples of operational plans are training plans, system deployment plans, and product design plans.

**Top-down approach**: **Upper (or senior) management** is responsible for initiating and defining policies for the organization. Security policies provide direction for all levels of the organization’s hierarchy. **Middle Management** flesh out the security policy into standards, baselines, guidelines, and procedures. The **operational managers** or **security processions** must then implement the configurations prescribed in the security management documentation. Finally, the **end users** must comply with all the security policies of the organization.

**Bottom-up approach**: the IT staff makes security decisions directly without input from senior management. It’s rarely used and is considered problematic in the IT industry.

**Security management** is a responsibility of **upper management**, not the **IT staff**, and is considered an issue of business operations rather than IT administration. The information security (InfoSec) team should be led by a designated (CISO) who reports directly to senior management, such as the CIO, CEO, or the board of directors.

Every security plan is **useless** without approval of senior management.

1. Organizational Processes
   1. Acquisitions and mergers place an organization at an increased level of risk. Such risks include inappropriate information disclosure, data loss, downtime, or failure to achieve sufficient return on investment (ROI).
2. Ethics (Chapter 19):
   1. Organizational Code of Ethics (for Government Service written into federal law):
      1. Put loyalty to the highest moral principles and to country above loyalty to persons, party, or Government department.
      2. Uphold the Constitution, laws, and regulations of the US and of all governments therein and never be a party to their evasion
      3. Give a full day’s labor for a full day’s pay; giving earnest effort and best thought to the performance of duties
      4. Seek to find and employ more efficient and economical ways of getting tasks accomplished
      5. Never discriminate unfairly by the dispensing of special favors or privileges to anyone, whether for remuneration or not; and never accept, for himself or herself or for family members, favors or benefits under circumstances which might be construed by reasonable persons as influencing the performance of governmental duties
      6. Make no private promises of any kind binding upon the duties of office, since a Government employee has no private word which can be binding on public duty.
      7. Engage in no business with the Government, either directly or indirectly, which is inconsistent with the conscientious performance of governmental duties
      8. Never use any information gained confidentially in the performance of governmental duties as a means of making private profit
      9. Expose corruption wherever discovered
      10. Uphold these principles, ever conscious that public office is a public trust
   2. (ISC)2 Code of Ethics (www.isc2.org/ethics):
      1. Code of Ethics Preamble:
         1. The safety and welfare of society and the common good, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
         2. Therefore, strict adherence to this Code is a condition of certification.
      2. Code of Ethics Canons:
         1. Protect society, the common good, necessary public trust and confidence, and the infrastructure.
         2. Act honorably, honestly, justly, responsibly, and legally
         3. Provide diligent and competent service to principals
         4. Advance and protect the profession
      3. Code of Ethics Complaints:
         1. Any member of the general public may file a complaint involving canons I or II.
         2. Only an employer or someone with a contracting relationship with the individual may file a complaint under canon III
         3. Other professionals may file a complaint under canon IV. It’s important to note that this is not limited to cybersecurity professionals. Anyone who is certified or licensed as a professional and subscribes to a code of ethics as part of that licensure or certification is eligible to file a canon IV complaint.
   3. Ethics and the Internet
      1. RFC 1087: these are unacceptable and unethical:
         1. Seeks to gain unauthorized access to the resources of the internet
         2. Disrupts the intended use of the internet
         3. Wastes resources (people, capacity, computer) through such actions
         4. Destroys the integrity of computer-based information
         5. Compromises the privacy of users
      2. Ten Commandments of Computer Ethics (cpsr.org/issues/ethics/cei):
         1. Thou shalt not use a computer to harm other people
         2. Thou shalt not interfere with other people’s computer work
         3. Thou shalt not snoop around in other people’s computer files
         4. Thou shalt not use a computer to steal
         5. Thou shalt not use a computer to bear false witness
         6. Thou shalt not copy proprietary software for which you have not paid
         7. Thou shalt not use other people’s computer resources without authorization or proper compensation
         8. Thou shalt not appropriate other people’s intellectual output
         9. Thou shalt think about the social consequences of the program you are writing or the system you are designing
         10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans
      3. Code of Fair Information Practices:
         1. There must be no personal data record-keeping systems whose very existence is secret
         2. There must be a way for a person to find out what information about the person is in a record and how it is used
         3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person’s consent
         4. There must be a way for a person to correct or amend a record of identifiable information about the person
         5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data

Chapter 3

1. Project Scope and Planning
   1. Perform a structured review of the business’s organization from a crisis planning point of view
      1. Operational departments that are responsible for the core services the business provides to its client
      2. Critical support services, such as the IT department, facilities and maintenance personnel, and other groups responsible for the upkeep of systems that support the operational departments
      3. corporate security teams responsible for physical security, since they are many times the first responders to an incident and are also responsible for the physical safeguarding of the primary facility and alternate processing facility
      4. senior executives and other key individuals essential for the ongoing viability of the organization
   2. Create a BCP team with the approval of senior management
      1. representatives from each of the organization's departments responsible for the core services performed by the business
      2. business unit team members from the functional areas identified by the organizational analysis
      3. IT subject-matter experts with technical expertise in areas covered by the BCP
      4. cybersecurity team members with knowledge of the BCP process
      5. Physical security and facility management teams responsible for the physical plant
      6. attorneys familiar with corporate legal, regulatory, and contractual responsibilities
      7. human resources team members who can address staffing issues and the impact on individual employees
      8. public relations team members who need to conduct similar planning for how they will communicate with stakeholders and the public in the event of a disruption
      9. senior management representatives with the ability to set the vision, define priorities, and allocate resources
   3. Assess the resources available to participate in business continuity activities
      1. **BCP Development** The BCP team will require some resources to perform the four elements of the BCP process (project scope and planning, business impact analysis, continuity planning, and approval and implementation). It's more than likely that the major resource consumed by this BCP phase will be effort expended by members of the BCP team and the support staff they call on to assist in the development of the plan
      2. **BCP Testing, Training, and Maintenance** The testing, training, and maintenance phases of BCP will require some hardware and software commitments. Still, once again, the major commitment in this phase will be the effort of the employees involved in those activities.
      3. **BCP Implementation** When a disaster strikes and the BCP team deems it necessary to conduct a full-scale implementation of the business continuity plan, the implementation will require significant resources. Those resources include a large amount of effort (BCP will likely become the focus of a large part, if not all, of the organization) as well as direct financial expenses. For this reason, the team must use its BCP implementation powers judiciously yet decisively.
   4. Analyze the legal and regulatory landscape that governs an organization’s response to a catastrophic event
      1. Be sure to keep your attorneys involved throughout the lifetime of your BCP, including the testing and maintenance phases.
      2. If your contracts include commitments to customers expressed as service-level agreements (SLAs), you might find yourself in breach of those contracts if a disaster interrupts your ability to service your clients. Many clients may feel sorry for you and want to continue using your products/services, but their own business requirements might force them to sever the relationship and find new suppliers
2. Business Impact Analysis
   1. Quantitative Impact Assessment: To begin the quantitative assessment, the BCP team should sit down and draw up a list of organization assets and then assign an asset value (AV) in monetary terms to each asset. The MTD is the maximum length of time a business function can tolerate a disruption before suffering irreparable harm. The recovery time objective (RTO) for each business function is the amount of time in which you think you can feasibly recover the function in the event of a disruption. The recovery point objective (RPO) is the data loss equivalent to the time-focused RTO. The RPO defines the point in time before the incident where the organization should be able to recover data.
   2. Qualitative Impact Assessment: The BCP team must sit down and discuss (preferably with the involvement of senior management) qualitative concerns: Loss of goodwill among your client base, Loss of employees to other jobs after prolonged downtime, Social/ethical responsibilities to the community, and Negative publicity. Qualitative concerns may justify elevating or lowering the priority of risks that already exist on the ALE-sorted quantitative list.
   3. A full listing of risks facing your organization will require input from all members of the BCP team. Be sure to gather input from all parts of the organization, especially from any areas not represented on the BCP team.
   4. The risk identification portion of the process is purely qualitative. At this point in the process, the BCP team should not be concerned about the likelihood that each type of risk will materialize or the amount of damage such an occurrence would inflict upon the continued operation of the business. The results of this analysis will drive both the qualitative and quantitative portions of the remaining BIA tasks.
   5. Remember that a contract is not normally sufficient due diligence when choosing a cloud provider. You should also verify that they have the controls in place to deliver on their contractual commitments. Although it may not be possible for you to physically visit the vendor's facilities to verify their control implementation, you can always do the next best thing-send someone else. The vendor may have already hired an independent auditing firm to conduct an assessment of its controls. They can make the results of this assessment available to you in the form of a Service Organizational Control (SOC) report.
3. Continuity Planning
   1. Strategy development: The BCP team must now take the prioritized list of concerns raised by the quantitative and qualitative resource prioritization exercises and determine which risks will be addressed by the business continuity plan. Fully addressing all the contingencies would require the implementation of provisions and processes that maintain a zero-downtime posture in the face of every possible risk. For obvious reasons, implementing a policy this comprehensive is impossible. The BCP team should look back to the MTD estimates created during the early stages of the BIA and determine which risks are deemed acceptable and which must be mitigated by BCP continuity provisions.
   2. Provisions and processes: 3 categories of assets must be protected through this stage:
      1. People: Management should provide team members with all the resources they need to complete their assigned tasks.
      2. Building/facilities
         1. Hardening Provisions
         2. Alternate Sites
      3. Infrastructure: The BCP must address how the organization will protect these systems against risks identified during the strategy development phase. There are two main methods of providing this protection:
         1. Physically Hardening Systems
         2. Alternative Systems
4. Approval and Implementation
   1. Plan Approval: If possible, you should attempt to have the plan endorsed by the top executive in your business-the CEO, chairperson, president, or similar business leader. It gives more credibility the eyes of other senior managers, who might otherwise brush it off as a necessary but trivial IT initiative.
   2. Plan Implementation
      1. Start implementing the plan with a clear schedule
      2. Make sure the plan is kept up to date
   3. Training and Education
      1. Everyone in the organization should receive at least a plan overview briefing. These briefings provide employees with the confidence that business leaders have considered the possible risks posed to the continued operation of the business and have put a plan in place to mitigate the impact on the organization should a disruption occur.
      2. Furthermore, at least one backup person should be trained for every BCP task to provide redundancy in the event personnel and injured or cannot reach the workplace during an emergency.
   4. BCP Documentation (by all BCP team member): to guide someone else if the senior BCP team members are not present to guide the effort, for historical record to understand the needs for changes, and for “sanity check”.
   5. Continuity Planning Goals: First, the plan should describe the goals of continuity planning as set forth by the BCP team and senior management. These goals should be decided on at or before the first BCP team meeting and will most likely remain unchanged throughout the life of the BCP. Most common goal is to ensure the continuous of the operation of the business in the face of an emergency. Other goals may be added for organizational needs.
   6. Statement of Importance: The statement of importance reflects the criticality of the BCP to the organization's continued viability. This document commonly takes the form of a letter to the organization's employees, stating the reason that the organization devoted significant resources to the BCP development process and requesting the cooperation of all personnel in the BCP implementation phase. If you can put out this letter under the signature of the CEO or an officer at a similar level, the plan will carry tremendous weight as you attempt to implement changes throughout the organization.
   7. Statement of Priorities: When listing priorities, you should also include a statement that they were developed as part of the BCP process and reflect the importance of the functions to continued business operations in the event of an emergency and nothing more. Otherwise, the list of priorities could be used for unintended purposes and result in a political turf battle between competing organizations to the detriment of the business continuity plan.
   8. Statement of Organizational Responsibility: The statement of organizational responsibility also comes from a senior-level executive and can be incorporated into the same letter as the statement of importance. It echoes the sentiment that "business continuity is everyone's responsibility!"
   9. Statement of Urgency and Timing: The statement of urgency and timing expresses the criticality of implementing the BCP and outlines the implementation timetable decided on by the BCP team and agreed to by upper management. The wording of this statement will depend on the actual urgency assigned to the BCP process by your organization's leadership. Consider including a detailed implementation timeline to foster a sense of urgency.
   10. Risk Assessment: Include the actual AV, EF, ARO, SLE, and ALE figures in the quantitative analysis. Also, describe the thought process behind the analysis to the reader. Keep in mind that the assessment reflects a point-in-time evaluation.
   11. Risk Acceptance/Mitigation: Business continuity planners should resist these statements and ask business leaders to document their risk acceptance decisions formally. If auditors later scrutinize your business continuity plan, they will most certainly look for formal artifacts of any risk acceptance decisions made in the BCP process.
       1. For risks that were deemed acceptable, it should outline the reasons the risk was considered acceptable as well as potential future events that might warrant a reconsideration of this determination.
       2. For risks that were deemed unacceptable, it should outline the risk management provisions and processes put into place to reduce the risk to the organization's continued viability.
   12. Vital Records Program: Sit down with functional leaders and ask, "If we needed to rebuild our organization today in a completely new location without access to any of our computers or files, what records would you need?" (asking the team). You should be able to identify the storage locations for each document identified in your vital records inventory.
   13. Emergency Response Guidelines: How the first employee to detect an emergency react? These guidelines should include the following:
       1. Immediate response procedures
       2. A list of the individuals to notify of the incident
       3. Secondary response procedures that first responders should take while waiting for the BCP team to assemble
   14. Maintenance: The BCP documentation and the plan itself must be living documents. The BCP team should not disband after the plan is developed but should still meet periodically to discuss the plan and review the results of plan tests to ensure that it continues to meet organizational needs. Keep in mind that drastic changes in an organization's mission or resources may require going back to the BCP drawing board and beginning again.
   15. Testing and Exercises: The BCP documentation should outline a formalized exercise program to ensure that the plan remains current.

Chapter 4

1. Criminal Law
   1. Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Identity Theft and Assumption Deterrence Act (among others) provide criminal penalties for serious cases of computer crime.
2. Civil Law
   1. Civil laws form the bulk of the U.S. body of laws. They are designed to provide for an orderly society and govern matters that are not crimes but that require an impartial arbiter to settle between individuals and organizations. Examples of the types of matters that may be judged under civil law include contract disputes, real estate transactions, employment matters and estate/probate procedures.
   2. Civil laws also are used to create the framework of government that the executive branch uses to carry out its responsibilities. These laws budgets for governmental activities and lay out the authority granted to the executive branch to create administrative laws.
   3. Civil laws are enacted in the same manner as criminal laws. They must pass through the legislative process before enactment and are subject to the same constitutional parameters and judicial review procedures. At the federal level, both criminal and civil laws are embodied in the United States Code (USC).
3. Administrative Law
   1. Executive branch agencies have some leeway to enact administrative law, in the form of executive orders, policies, procedures, and regulations that govern the daily operations of the agency. Administrative law is published in the Code of Federal Regulations (CFR).
4. Computer Crime

Because of the global reach of the internet, most computer crimes cross state lines and, therefore, fall under federal jurisdiction and are prosecuted in the federal court system. However, in some circumstances, state laws can be more restrictive than federal laws and impose harsher penalties.

* 1. Computer Fraud and Abuse Act (CFAA):
     1. Access classified information or financial information in a federal system without authorization or in excess of authorized privileges
     2. Access a computer used exclusively by the federal government without authorization
     3. Use a federal computer to perpetrate a fraud (unless the only object of the fraud was to gain use of the computer itself)
     4. Cause malicious damage to a federal computer system in excess of $1,000
     5. Modify medical records in a computer when doing so impairs or may impair the examination, diagnosis, treatment, or medical care of an individual
     6. Traffic in computer passwords if the trafficking affects interstate commerce or involves a federal computer system

The threshold of damage was raised to $5,000:

1. Any computer used exclusively by the U.S. government
2. Any computer used exclusively by a financial institution
3. Any computer used by the government or a financial institution when the offense impedes the ability of the government or institution to use that system
4. Any combination of computers used to commit an offense when they are not all located in the same state

National Information Infrastructure Protection Act of 1996:

* + 1. Broadens the CFAA to cover computer systems used in international commerce in addition to systems used in interstate commerce
    2. Extends similar protections to portions of the national infrastructure other than computing systems, such as railroads, gas pipelines, electric power grids, and telecommunications circuits
    3. Treats any intentional or reckless act that causes damage to critical portions of the national infrastructure as a felony
  1. Federal Sentencing Guidelines
     1. The guidelines formalized the prudent person rule, which requires senior executives to take personal responsibility for ensuring the due care that ordinary, prudent individuals would exercise in the same situation.
     2. The guidelines allowed organizations and executives to minimize punishment for infractions by demonstrating that they used due diligence in the conduct of their information security duties
     3. The guidelines outlined three burdens of proof for negligence: First, the person accused of negligence must have a legally recognized obligation. Second, the person must have failed to comply with recognized standards. Finally, there must be a causal relationship between the act of negligence and subsequent damages
  2. Federal Information Security Management Act

FISMA requires federal agencies implement an information security program that covers the agency's operations and government agencies include the activities of contractors in their security management programs. It replaces Computer Security Act of 1987 and Government Information Security Reform Act of 2000. NIST (responsible for developing the FISMA implementation guidelines) outlines the following elements for effective information security program:

* + 1. Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization
    2. Policies and procedures that are based on risk assessments, cost-effectively reducing information security risks to an acceptable level and ensuring that information security is addressed throughout the lifecycle of each organizational information system
    3. Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.
    4. Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks
    5. Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually
    6. A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization
    7. Procedures for detecting, reporting, and responding to security incidents
    8. Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization
  1. Federal Cybersecurity Laws of 2014

The first of these was the confusingly named Federal Information Systems Modernization Act (also bearing the acronym FISMA). The 2014 FISMA modified the rules of the 2002 FISMA by centralizing federal cybersecurity responsibility with the Department of Homeland Security. There are two exceptions to this centralization: defense-related cybersecurity issues remain the responsibility of the secretary of defense, and the director of national intelligence bears responsibility for intelligence-related issues.

Second, Congress passed the Cybersecurity Enhancement Act, which charges NIST with responsibility for coordinating nationwide work on voluntary cybersecurity standards. NIST produces the 800 series of Special Publications related to computer security in the federal government.

The following are commonly used NIST standards:

* + 1. NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. This standard is required for use in federal computing systems and is also commonly used as an industry cybersecurity benchmark.
    2. NIST SP-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Compliance with this standard's security controls (which are quite similar to those found in NIST 800-53) is often included as a contractual requirement by government agencies. Federal contractors must often comply with NIST SP 800-171
    3. The NIST Cybersecurity Framework (CSF) is a set of standards designed to serve as a voluntary risk-based framework for securing information and systems.
  1. Intellectual Property (IP)

Many products depend on secret recipes or production techniques-take the legendary secret formula for Coca-Cola or KFC's secret blend of herbs and spices, for example.

These intangible assets are collectively referred to as intellectual property (IP). We'll explore the laws surrounding the four major types of intellectual property-copyrights, trademarks, patents, and trade secrets.

* + 1. Copyright and the Digital Millennium Copyright Act

Eight board categories of works qualify for copyright protection:

* + - 1. Literary works
      2. Musical works
      3. Dramatic works
      4. Pantomimes and choreographic works
      5. Pictorial, graphical, and sculptural works
      6. Motion pictures and other audiovisual works
      7. Sound recordings
      8. Architectural works

There has been some question over whether copyrights can be extended to cover the "look and feel" of a software package's graphical user interface. If you will be involved in this type of issue, you should consult a qualified intellectual property attorney to determine the current state of legislation and case law.

There's a formal procedure to obtain a copyright that involves sending copies of the protected work along with an appropriate registration fee to the U.S. Copyright Office. However, officially registering a copyright is not a prerequisite for copyright enforcement. Indeed, the law states that the creator of a work has an automatic copyright from the instant the work is created. If you can prove in court that you were the creator of a work (perhaps by publishing it), you will be protected under copyright law. Official registration merely provides the government's acknowledgment that they received your work on a specific date.

Copyright ownership always defaults to the creator of a work. The exceptions to this policy are works for hire. For example, when an employee in a company's public relations department writes a press release, the press release is considered a work for hire. A work may also be considered a work for hire when it's made as part of a written contract declaring it as such.

Current copyright law provides for a lengthy period of protection. Works by one or more authors are protected until 70 years after the death of the last surviving author. Works for hire and anonymous works are provided protection for 95 years from the date of first publication or 120 years from the date of creation, whichever is shorter.

The Digital Millennium Copyright Act (DMCA) serves to bring U.S. copyright law into compliance with terms of two World Intellectual Property Organization (WIPO) treaties. The first major provision of the DMCA provides for penalties of up to $1 million and 10 years in prison for repeat offenders. Nonprofit institutions such as libraries and schools are exempted from this provision.

The DMCA also limits the liability of internet service providers (ISPs) when their circuits are used by criminals violating the copyright law. To qualify for this exemption, the service provider's activities must meet the following requirements (quoted directly from the Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, December 1998):

1. The transmission must be initiated by a person other than the provider
2. The transmission, routing, provision of connections, or copying must be carried out by an automated technical process without selection of material by the service provider.
3. The service provider must not determine the recipients of the material
4. Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients and must not be retained for longer than reasonably necessary.
5. The material must be transmitted with no modification to its content.

The DMCA also exempts activities of service providers related to system caching, search engines, and the storage of information on a network by individual users. However, in those cases, the service provider must take prompt action to remove copyrighted materials upon notification of the infringement.

The DMCA spells out the application of copyright law principles to the streaming of audio and/or video content over the internet. The DMCA states that these uses are to be treated as "eligible nonsubscription transmissions."

* + 1. Trademarks

If you use a trademark in the course of your public activities, you are automatically protected under any relevant trademark law and can use the TM symbol to show that you intend to protect words or slogans as trademarks. If you want official recognition of your trademark, you can register it with the United States Patent and Trademark Office (USPTO). This process generally requires an attorney to perform a due diligence comprehensive search for existing trademarks that might preclude your registration. The entire registration process can take more than a year from start to finish. Once you've received your registration certificate from the USPTO, you can denote your mark as a registered trademark with the R symbol.

"Intent to use" application is that you register a trademark that you intend to use but are not necessarily already using.

The acceptance of a trademark application in the United States depends on these two main requirements:

* + - 1. The trademark must not be confusingly similar to another trademark-you should determine this during your attorney's due diligence search. There will be an open opposition period during which other companies may dispute your trademark application.
      2. The trademark should not be descriptive of the goods and services that you will offer. For example, "Mike's Software Company" would not be a good trademark candidate because it describes the product produced by the company. The USPTO may reject an application if it considers the trademark descriptive.

In the United States, trademarks are granted for an initial period of 10 years and can be renewed for unlimited successive 10-year periods.

* + 1. Patents

Utility patents protect the intellectual property rights of inventors. They provide a period of 20 years from the time of the invention (from the date of initial application) during which the inventor is granted exclusive rights to use the invention (whether directly or via licensing agreements). At the end of the patent exclusivity period, the invention is in the public domain available for anyone to use.

Patents have three main requirements:

* + - 1. The invention must be new. Inventions are patentable only if they are original ideas.
      2. The invention must be useful. It must actually work and accomplish some sort of task.
      3. The invention must not be obvious. You could not, for example, obtain a patent for your idea to use a drinking cup to collect rainwater. This is an obvious solution. You might, however, be able to patent a specially designed cup that optimizes the amount of rainwater collected while minimizing evaporation.

Patent Trolls: Some companies don't actually build anything or use the patents they own. Instead, they make money by suing other companies for using similar ideas. They just hold the patents to threaten legal action and get paid settlements.

* + 1. Trade Secrets

Two of the previously discussed intellectual property tools-copyrights and patents-could be used to protect this type of information, but with these two major disadvantages:

* + - 1. Filing a copyright or patent application requires that you publicly disclose the details of your work or invention. This automatically removes the "secret" nature of your property and may harm your firm by removing the mystique surrounding a product or by allowing unscrupulous competitors to copy your property in violation of international intellectual property laws.
      2. Copyrights and patents both provide protection for a limited period of time. Once your legal protection expires, other firms are free to use your work at will (and they have all the details from the public disclosure you made during the application process!).

There actually is an official process regarding trade secrets. By their nature you don't register them with anyone; you keep them to yourself. You must ensure that anyone who does have this type of access is bound by a nondisclosure agreement (NDA) that prohibits them from sharing the information with others and provides penalties for violating the agreement.

Patent law doesn't provide adequate protection for computer software products. Copyright law protect only the actual text of the source code and doesn't prohibit others from rewriting your code in a different form and accomplishing the same objective.

Economic Espionage Act of 1996 has these two major provisions:

Anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years.

Anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years.

* 1. Licensing

Four common types of license agreements are in use today:

* + 1. **Contractual license** agreements use a written contract between the software vendor and the customer, outlining the responsibilities of each. These agreements are commonly found for high-priced and/or highly specialized software packages.
    2. **Shrink-wrap** licensing agreements are written on the outside of the software packaging. They commonly include a clause stating that you acknowledge agreement to the terms of the contract simply by breaking the shrink-wrap seal on the package
    3. **Click-through** (also known as browser wrap) license agreements are becoming more commonplace than shrink-wrap agreements. In this type of agreement, the contract terms are either written on the software box or included in the software documentation. During the installation process, you are required to click a button indicating that you have read the terms of the agreement and agree to abide by them. This adds an active consent to the process, ensuring that the individual is aware of the agreement's existences prior to installation.
    4. **Cloud services** license agreements take click-through agreements to the extreme. Most cloud services do not require any form of written agreement and simply flash legal terms on the screen for review. In some cases, they may provide a link to legal terms and a check box for users to confirm that they read and agree to the terms. Most users, in their excitement to access a new service, simply click their way through the agreement without reading it and may unwittingly bind their entire organization to onerous terms and conditions.

Industry groups provide guidance and enforcement activities regarding software licensing. You can get more information from their websites. One major group is the Software Alliance.

* 1. Import/Export

Two sets of federal regulations governing imports and exports are of particular interest to cybersecurity professionals:

* + 1. The international Traffic in Arms Regulations (ITAR) controls the export of items that are specifically designated as military and defense items, including technical information related to those items. The item covered under ITAR appear on a list called the United States Munitions List (USML), maintained in 22 CFR 121.
    2. The Export Administration Regulations (EAR) cover a broader set of items that are designed for commercial use but may have military applications. Items covered by EAR appear on the Commerce Control List (CCL) maintained by the U.S. Department of Commerce. Notably, EAR includes an entire category covering information security products.
  1. Countries of Concern

Currently, U.S. firms can export high-performance computing systems to virtually any country without receiving prior approval from the government. There are exceptions to this rule for countries designated by the Department of Commerce's Bureau of Industry and Security (BIS) as countries of concern based on the fact that they pose a threat of nuclear proliferation, they are classified as state sponsors of terrorism, or other concerns. These countries include North Korea, Sudan, and Syria.

* 1. Encryption Export Controls

After a lengthy lobbying campaign by the software industry, the president directed the Commerce Department to revise its regulations to foster the growth of the American security software industry (it was treated like a weapon due to potential military purposes).

Security software is now divided into "retail" and "mass market" categories.

By regulation, this review should be completed within 30 days. Once approved, companies can export the software freely. In practice, government review often take longer than the 30-day legal deadline. Companies facing delays may either wait indefinitely or take the matter to court to force a decision.

* 1. Privacy

The main source of this contention is that the Constitution's Bill of Rights does not explicitly provide for a right to privacy. However, this right has been upheld by numerous courts and is vigorously pursued by organizations such as the American Civil Liberties Union (ACLU).

Europeans have also long been concerned with their privacy.

* + 1. **Fourth Amendment** to the U.S. Constitution. It reads as follows: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
    2. **The Privacy Act of 1974** (later amended by the bellow act) applies only to government agencies (not all organizations): The Privacy Act mandates that agencies maintain only the records that are necessary for conducting their business and that they destroy those records when they are no longer needed for a legitimate function of government. It provides a formal procedure for individuals to gain access to records the government maintains above them and to request that incorrect records be amended.
    3. **Electronic Communications Privacy Act of 1986**: It prohibits the interception or disclosure of electronic communication and defines those situations in which disclosure is legal (a fine of up to $500 and a prison term of up to five years).
    4. **Communications Assistance for Law Enforcement Act (CALEA) of 1994**: requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order.
    5. **Economic Espionage Act of 1996**: extends the definition of property to include proprietary economic information so that the theft of this information can be considered industrial or corporate espionage.
    6. **Health Insurance Portability and Accountability Act of 1996** (**HIPAA**, later amended by HITECH): Among the provisions of HIPAA are privacy and security regulations requiring strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store private medical information about individuals. HIPAA-covered entities that experience a data breach must notify affected individuals of the breach and must also notify both the secretary of health and human services and the media when the breach affects more than 500 individuals. Any relationship between a covered entity and a business assocciate must be governed by a written contract known as a business associate agreement (BAA). Business associates are directly subject to HIPAA and HIPAA enforcement actions.
    7. **Health Information Technology for Economic and Clinical Health Act of 2009: update privacy and security requirements** (**HITECH**, implemented through the HIPAA Omnibus Rule in 2013)
    8. Data breach notification law (SB 1386) include: SSN, Drier's license number, state identification card number, credit or debit card number, bank account number (including security code, access code, or password), medical records, health insurance information.
    9. Children's Online Privacy Protection Act of 1998 (COPPA):
       1. Websites must have a privacy notice that clearly states the type of information they collect and what it's used for, including whether any information is disclosed to third parties. The privacy notice must also include contact information for the operators of the site.
       2. Parents must be provided with the opportunity to review any information collected from their children and permanently delete it from the site's records.
       3. Parents must give verifiable consent to the collection of information about children younger than the age of 13 prior to any such collection. Exceptions in the law allow websites to collect minimal information solely for the purpose of obtaining such parental consent.
    10. Gramm-Leach Bliley Act of 1999:

Until the Gramm-Leach-Bliley Act (GLBA) became law in 1999, there were strict governmental barriers between financial institutions. GLBA somewhat realized the regulations concerning the services each organization could provide. When Congress passed this law, it realized that this increased latitude could have far-reaching privacy implications. Because of this concern, it included a number of limitations on the types of information that could be exchanged even among subsidiaries of the same corporation and required financial institutions to provide written privacy policies to all their customers.

* + 1. USA PATRIOT Act of 2001

Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 in direct response to the September 11, 2001, f attacks in New York City and Washington, DC.

* + - 1. Authorities can now get one warrant to monitor all communications for a single person (including multiple phones, computers, etc.)
      2. The government can access detailed user activity data using a subpoena, which is easier to get than a wiretap.
      3. The USA PATRIOT Act amends the Computer Fraud and Abuse Act (yes, another set of amendments!) to provide more severe penalties for criminal acts. The PATRIOT Act provides for jail terms of up to 20 years and once again expands the coverage of the CFAA.
    1. Family Educational Rights and Privacy Act (FERPA)

It grants certain privacy rights to students older than 18 and the parents of minor students.

* + - 1. Parents/students have the right to inspect any educational records maintained by the institution on the student.
      2. Parents/students have the right to request correction of records they think are erroneous and the right to include a statement in the records contesting anything that is not corrected.
      3. Schools may not release personal information from student records without written consent, except under certain circumstances.
    1. Identity Theft and Assumption Deterrence Act

In the past, the only legal victims of identity theft were the creditors who were defrauded. This act makes identity theft a crime against the person whose identity was stolen and provides severe criminal penalties (up to a 15-year prison term and/or a $250,000 fine) for anyone found guilty of violating this law.

If you're planning to monitor the communications of your employees, you should take reasonable precautions to ensure that there is no implied expectation of privacy. Here are some common measures to consider:

1. Clauses in employment contracts that state the employee has no expectation of privacy while using corporate equipment
2. Similar written statements in corporate acceptable use and privacy policies
3. Logon banners warning that all communications are subject to monitoring
4. Warning labels on computers and telephones warning of monitoring
   * 1. European Union Privacy Law

The European Union (EU) has served as a leading force in the world of information privacy, passing a series of regulations designed to protect individual privacy rights. These laws function in a comprehensive manner, applying to almost all individually identifiable information, unlike U.S. privacy laws, which generally apply to specific industries or categories of information

* + - 1. European Union Data Protection Directive (DPD)

On October 24, 1995, the European Parliament passed a sweeping Data Protection Directive (DPD) outlining privacy measures that must be in place for protecting personal data processed by information systems. The directive went into effect three years later in October 1998, serving as the first broad-based privacy law in the world. The DPD required that all processing of personal data meet one of the following criteria:

* + - * 1. Consent
        2. Contract
        3. Legal obligation
        4. Vital interest of the data subject
        5. Balance between the interests of the data holder and the interests of the data subject

The directive also outlined key rights of individuals about whom data is held and/or processed:

1. Right to access the data
2. Right to know the data's source
3. Right to correct inaccurate data
4. Right to withhold consent to process data in some situations
5. Right of legal action should these rights be violated

The passing of the DPD forced organizations around the world, even those based outside Europe, to consider their privacy obligations due to transborder data flow requirements.

* + - 1. European Union General Data Protection Regulation (GDPR)

The new law applies to all organizations that collect data from EU residents or process that information on behalf of someone who collects it (major difference from DPD). The key provisions of the GDPR include the following:

* + - * 1. Lawfulness, fairness, and transparency says that you must have a legal basis for processing personal information, you must not process data in a manner that is misleading or detrimental to data subjects, and you must be open and honest about data processing activities.
        2. Purpose limitation says that you must clearly document and disclose the purposes for which you collect data and limit your activity to disclosed purposes.
        3. Data minimization says that you must ensure that the data you process is adequate for your stated purpose and limited to what you actually need for that purpose.
        4. Accuracy says that the data you collect, create, or maintain is correct and not misleading, that you maintain updated records, and that you correct or erase inaccurate data.
        5. Storage limitation says that you keep data only for as long as it is needed to fulfill a legitimate, disclosed purpose and that you comply with the "right to be forgotten" that allows people to require companies to delete their information if it is no longer needed.
        6. Security says that you must have appropriate integrity and confidentiality controls in place to protect data.
        7. Accountability says that you must take responsibility for actions you take with protected data and that you must be able to demonstrate your compliance.
      1. Cross-Border Information Sharing

Organizations needing to conduct transfers between their subsidiaries have two options available for complying with EU regulations:

* + - * 1. Organizations may adopt a set of standard contractual clauses that have been approved for use in situations where information is being transferred outside of the EU. Those clauses are found on the EU website and are available for integration into contracts.
        2. Organizations may adopt binding corporate rules that regulate data transfers between internal units of the same firm. This is a very time-consuming process-the rules must be approved by every EU member nation where they will be used, to typically this path is only adopted by very large organizations.

Privacy Shield (now invalid) used to be an agreement between the U.S. and the EU to make data sharing easier. Companies had to prove they followed privacy rules to earn the "Privacy Shield". In 2020, the European Court of Justice struck it down in the Schrem II case.

In some cases, conflicts arise between laws of different nations. For example, electronic discovery rules in the United States might require the production of evidence that is protected under GDPR. In those cases, privacy professionals should consult with attorneys to identify an appropriate course of action.

The Asia-Pacific Economic Cooperation (APEC) publishes a privacy framework that incorporates many standard privacy practices, such as preventing harm, notice, consent, security, and accountability. This framework is used to promote the smooth cross-border flow of information between APEC member nations.

* + 1. Canadian Privacy Law

The Personal Information Protection and Electronic Documents Act (PIPEDA) is a national-level law that restricts how commercial businesses may collect, use, and disclose personal information.

Generally speaking, PIPEDA covers information about an individual that is identifiable to that individual. The Canadian government provides the following examples of information covered by PIPEDA:

* + - 1. Race, national, or ethnic origin
      2. Religion
      3. Age
      4. Marital status
      5. Medical, education, or employment history
      6. Financial information
      7. DNA
      8. Identifying numbers
      9. Employee performance records

The law excludes information that does not fit the definition of personal information, including the following examples provided by the Information Commissioner of Canada:

1. Information that is not about an individual, because the connection with a person is too weak or far-removed
2. Information about an organization such as a business
3. Information that has been rendered anonymous, as long as it is not possible to link that data back to an identifiable person
4. Certain information about public servants such as their name, position, and title
5. A person's business contact information that an organization collects, uses, or discloses for the sole purpose of communicating with that person in relation to their employment, business, or profession

PIPEDA generally does not apply to nonprofit organizations, municipalities, universities, schools, and hospitals

1. State Privacy Laws

The California Consumer Privacy Act (CCPA) is an excellent example of this principle in action. California passed this sweeping privacy law in 2018, modeling it after the European Union's GDPR. Provisions of the law went into effect in 2020, providing consumers with the following:

* + - 1. The right to know what information businesses are collecting about them and how the organization uses and shares that information
      2. The right to be forgotten, allowing consumers to request that the organization delete their personal information, in some circumstances
      3. The right to opt out of the sale of their personal information
      4. The right to exercise their privacy rights without fear of discrimination or retaliation for their use

1. Compliance

PCI DSS has 12 main requirements.

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Protect all systems against malware and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications
7. Restrict access to card holder data by business need-to-know.
8. Identify and authenticate access to system components.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

Organizations that are not merchants but that store, process, or transmit credit card information on behalf of merchants must also comply with PCI DSS.

Dealing with the many overlapping, and sometimes contradictory, compliance requirements facing an organization requires careful planning. Many organizations employ full-time IT compliance staff responsible for tracking the regulatory environment, monitoring controls to ensure ongoing compliance, facilitating compliance audits, and meeting the organization's compliance report obligations

Organizations may be subject to compliance audits, either by their standard internal and external auditors or by regulators or their agents. Some regulations, such as PCI DSS, may require the organization to retain approved independent auditors to verify controls and provide a report directly to regulators.

In addition to formal audits, organizations often must report regulatory compliance to a number of internal and external stakeholders. For example, an organization's board of directors (or, more commonly, that board's audit committee) may require periodic reporting on compliance obligations and status. Similarly, PCI DSS requires organizations that are not compelled to conduct a formal third-party audit to complete and submit a self-assessment report outlining their compliance status.

1. Contracting and Procurement

The increased use of cloud services and other external vendors to store, process, and transmit sensitive information leads organizations to a new focus on implementing security reviews and controls in their contracting and procurement processes.

These are some questions to cover during these vendor governance reviews:

1. What types of sensitive information are stored, processed, or transmitted by the vendor?
2. What controls are in place to protect the organization's information?
3. How is your organization's information segregated from that of other clients?
4. If encryption is relied on as a security control, what encryption algorithms and key lengths are used? How is key management handled?
5. What types of security audits does the vendor perform, and what access does the client have to those audits?
6. Does the vendor rely on any other third parties to store, process, or transmit data? How do the provisions of the contract related to security extend to those third parties?
7. Where will data storage, processing, and transmission take place? If outside the home country of the client and/or vendor, what implications does that have?
8. What is the vendor's incident response process, and when will clients be notified of a potential security breach?
9. What provisions are in place to ensure the ongoing integrity and availability of client data?

Chapter 5: Protecting Security of Assets

The Asset Security domain focuses on collecting, handling, and protecting information throughout its lifecycle. A primary step in this domain is classifying information based on its value to the organization. All follow-on actions vary depending on the classification. For example, highly classified data requires stringent security controls. In contrast, unclassified data uses fewer security controls.

1. Identifying and Classifying Information and Assets

Organizations often include classification definitions within a security policy. Personnel then label assets appropriately based on the security policy requirements.

* 1. Sensitive data

Sensitive data is any information that isn't public or unclassified. It can include confidential, proprietary, protected, or any other type of data that an organization needs to protect due to its value to the organization, or to comply with existing laws and regulations.

* 1. Personally Identifiable Information

Personally identifiable information (PII) is any information that can identify an individual. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122 provides a more formal definition:

Any information about an individual maintained by an agency, including

* + 1. any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and
    2. any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Protection for personally identifiable information (PII) drives privacy and confidentiality requirements for rules, regulations, and legislation worldwide (especially in North America and the European Union). NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), provides more information on how to protect PII. It's available from the NIST SP \*800 Series) download page.

* 1. Protected Health Information

Protected health information (PHI) is any health-related information that can be related to a specific person. HIPAA mandates PHI protection. HIPAA provides a more formal definition of PHI:

Health information means any information, whether oral or recorded in any form or medium, that-

* + 1. is created or received by a heath care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
    2. relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
  1. Proprietary Data

Proprietary data refers to any data that helps an organization maintain a competitive edge. It could be software code it developed, technical plans for products, internal processes, intellectual property, or trade secrets.

1. Defining Data Classifications

Organizations typically include data classifications in their security policy or a data policy. The U.S. government provides clear definitions for these classifications. As you read them, note that the wording of each definition is close except for a few keywords. \*Top secret\* uses the phrase "exceptionally grave damage," \*secret\* uses the phrase "serious damage," and confidential uses "damage":

* 1. Top Secret The top secret label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe."
  2. Secret The secret label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe."
  3. Confidential The confidential label is "applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe."
  4. Unclassified Within the United States, unclassified data is available to anyone, though it often requires individuals to request the information using procedures identified in the Freedom of Information Act (FOIA).
     1. There are additional subclassifications of unclassified, such as for official use only (FOUO) and sensitive but unclassified (SBU). Documents with these designations have strict controls limiting their distribution. As an example, the U.S. Internal Revenue Service (IRS) uses SBU for individual tax records, restricting access to these records.

These classifications also apply to hardware assets. This includes any computing system or media that processes or holds this data.

Nongovernmental organizations rarely need to classify their data based on potential damage to national security. Some nongovernmental organizations use labels such as Class 3, Class 2, Class 1, and Class 0. Other organizations use more meaningful labels such as confidential (or proprietary), private, sensitive, and public

* 1. Confidential or Proprietary As an example. attackers have repeatedly attacked Sony, stealing more than 100 terabytes of data, including full-length versions of unreleased movies. These quickly showed up on file-sharing sites, and security experts estimated that people downloaded these movies up to a million times. The movie were proprietary, and the organization might have considered it exceptionally grave damage.
  2. Private Many organizations label PII and PHI data as private. It's also common to label internal employee data and some financial data as private. As an example, the payroll department of a company would have access to payroll data, but this data is not available to regular employees.
  3. Sensitive As an example, IT personnel within an organization might have extensive data about the internal network, including the layout, devices, operating systems, software, Internet Protocol (IP) addresses, and more. If attackers have easy access to this data, it makes it much easier for them to launch attacks.
  4. Public Although an organization doesn't protect the confidentiality of public data, it does take steps to protect its integrity.

For the CISSP exam, remember that "sensitive information" typically refers to any information that isn't public or unclassified

3. Defining Asset Classifications

A computer is processing top secret data, the computer should also be classified as a top secret asset.

4. Understanding Data States

* 1. Data at Rest system hard drives, solid-state drives (SSDs), external USB drives, storage area networks (SANs), and backup tapes. Strong symmetric encryption protects data at rest
  2. Data in Transit A combination of symmetric and asymmetric encryption protects data in transit
  3. Data in Use It's important to flush these buffers when the data is no longer needed. In some cases, it's possible for an application to work on encrypted data using homomorphic encryption

5. Determining Compliance Requirements

Some organizations have created a formal position called a compliance officer. The person filling this role ensures that the organization is conducting all business activities by following the laws and regulations that apply to the organization. This starts by first determining everywhere the organization operates, and what compliance requirements apply.

6. Determining Data Security Controls

Security administrators use the requirements defined in the security policy to identify security controls. For Table 5.1, the primary security control is strong encryption using AES 256. Administrators should identify methodologies, making it easy for employees to meet the requirements.

Several software companies sell a range of products that organizations can use to automate these tasks. Users apply relevant labels to emails before sending them. These emails pass through a data loss prevention (DLP) server that detects the labels and applies the required protection.

Any type of data that your organization wants to protect needs similar security definitions. For example, you should define requirements for data stored on assets such as servers, data backups stored onsite and offsite, and proprietary data.

Additionally, IAM security controls help ensure that only authorized personnel can access resources. Chapter 13, "Managing Identity and Authentication," and Chapter 14, "Controlling and Monitoring Access," cover identity and access management security controls in more depth.

7. Establishing Information and Asset Handling Requirements

* 1. Data Maintenance

Refers to ongoing efforts to organize and care for data throughout its lifetime.

If an organization stores all sensitive data on one server, it is relatively easy to apply all the appropriate controls to this one server.

Techniques such as air gaps ensure the two networks never physically touch each other: one network processes unclassified data only and another network processes classified data, for example. Additionally, the classified network can't access the internet, and internet attackers can't access it.

There are times when personnel need to add data to the classified network (updates as an example):

* + 1. One way is manual; personnel copy the data from the unclassified network to a USB device and carry it to the classified network.
    2. Another method is to use a unidirectional network bridge (data travel in only one direction).
    3. A third method is to use a technical guard solution, which is a combination of hardware and software placed between the two networks. A guard solution allows properly marked data to travel between the two networks.
  1. Data Loss Prevention (DLP)

DLP systems attempt to detect and block data exfiltration attempts. For example, imagine that your organization uses data classifications. A DLP system can scan files for these words and detect them.

Pattern-matching DLP systems look for specific patterns. The DLP can look for this pattern and detect it. Cloud-based DLP systems can look for the same code words or strings.

There are two primary types of DLP systems:

* + 1. Network-Based DLP: Administrators place it on the edge of the network to scan all data leaving the organization. The DLP system will send an alert, such as an email to an administrator. Cloud-based DLP is a subset of network-based DLP.
    2. Endpoint-Based DLP: An endpoint-based DLP can scan files stored on a system as well as files sent to external devices, such as printers. For example, an organization's endpoint-based DLP can prevent users from copying sensitive data to USB flash drives or sending sensitive data to a printer. It's also possible to configure an endpoint-based DLP system to regularly scan files (such as on a file server) for files containing specific keywords or patterns, or even for unauthorized file types, such as MP3 files.

Most DLP solutions also include discovery capabilities. The goal is to discover the location of valuable data within an internal network.

As an example, a database server may include unencrypted credit card numbers. When the DLP discovers and reports this database administrators can ensure the numbers are encrypted. As another example, company policy may dictate that employee laptops do not contain any PII data. A DLP content discovery system can search these and discover any unauthorized data. Additionally, many content discovery systems can search cloud resources used by an organization.

* 1. Marking Sensitive Data and Assets

Marking includes both physical and electronic marking and labels.

* + 1. Physical labels remain on the system or media throughout its lifetime.
    2. Digital marks or labels can be including the classification as a header or footer in a document or embed it as a watermark. It can help DLP systems to detect. Some DLP systems will also add metadata tags to the document when they detect that the document is classified.

Some organizations mandate specific desktop backgrounds on their computers. For example, a system used to process proprietary data might have a black desktop background with the word Proprietary in white and a wide orange border.

In many secure environments, personnel also use labels for unclassified media and equipment. If the organization marks unclassified data, too, unlabeled media would be easily noticeable, and the user would view an unmarked tape with suspicion.

Organizations often identify procedures to downgrade media. For example, if a backup tape includes confidential information, an administrator might want to downgrade the tape to unclassified. After administrator purge the tape, they can then downgrade it. It's rare to downgrade a system. In any event, approved procedures would need to be created to inform personnel what can be downgraded and what should be destroyed. It's often safer and easier just to purchase new media or equipment rather than follow through with the sanitization steps for reuse.

* 1. Handling Sensitive Information and Assets

Handling refers to the secure transportation of media through its lifetime.

A common occurrence is the loss of control of backup tapes. Backup tapes should be protected with the same level of protection as the data that they contain.

Data stored in the cloud needs to be protected with the same level of protection with which it is protected on site. Amazon Web Services (AWS) Simple Storage Service (S3) is one of the largest cloud service providers. Data is stored in AWS buckets, which are like folders on Windows systems. Unfortunately, this concept eludes many AWS users. As an example, a bucket owned by THSuite, a cannabis retailer, exposed the PII of more than 30,000 individuals in early 2020. Another example from 2020 involved 900,000 before and after cosmetic surgery images and videos stored in an unsecured bucket.

Chapter 17, "Preventing and Responding to Incidents," discusses the importance of logging, monitoring, and auditing. These controls verify that sensitive information is handled appropriately before a significant loss occurs. If a loss does occur, investigators use audit trails to help discover what went wrong. Any incidents that occur because personnel didn't handle data appropriately should be quickly investigated and actions taken to prevent a reoccurrence.

* 1. Data Collection Limitation

The guideline is clear. If the data doesn't have a clear purpose for use, don't collect it and store it. This is also why many privacy regulations mention limiting data collection.

* 1. Data Location

Data location refers to the location of data backups or data copies. A best practice is to keep a backup copy on site and another backup copy off site. When using cloud storage for backups, some organizations may need to verify the location of the cloud storage to ensure it is in a separate geographical location.

* 1. Storing Sensitive Data

Sensitive data should be stored in such a way that it is protected against any type of loss. Encryption methods prevent unauthorized entities from accessing the data even if they obtain databases or hardware assets.

Additionally, environmental controls protect the media. This includes temperature and humidity controls such as heating, ventilation, and air-conditioning (HVAC) systems.

The value of any sensitive data is much greater than the value of the media holding the sensitive data. It's cost-effective to purchase high-quality media, especially if the data will be stored for a long time, such as on backup tapes. Similarly, the purchase of high-quality USB flash drives with built-in encryption is worth the cost. Some of these USB flash drives include biometric authentication mechanisms using fingerprints, which provide added protection.

* 1. Data Destruction

An organization's security policy or data policy should define the acceptable methods of destroying data based on the data's classification. For example, an organization may require the complete destruction of media holding highly classified data, but allow personnel to use software tools to overwrite data files classified at a lower level.

NIST SP 800-88 Rev. 1, "Guidelines for Media Sanitization," provides comprehensive details on different sanitization methods. Sanitization methods (such as clearing, purging, and destroying) help ensure that data cannot be recovered. Proper sanitization steps remove all sensitive data (like removing SSDs, CDs/DVDs, and USB drives) before disposing of a computer.

Sanitization can also refer to using a trusted method to purge classified data from the media without destroying it.

* 1. Eliminating Data Remanence

Data remanence is the data that remains on media after the data was supposedly erased (residual magnetic flux or slack space for example). It may includes any type of private and sensitive data.

**Slack** space is the unused space within a disk cluster. Operating systems store files on hard disk drives in clusters, which are groups of sectors (the smallest storage unit on a hard disk drive). Imagine a cluster size of 4,096 bytes and a file size of 1,024 bytes. After storing the file, the cluster would have 3,072 bytes of slack space.

Some operating systems fill this slack space with data from memory. That's why personnel should never process classified data on unclassified systems. Sophisticated users can also hide data within slack space using tools such as `**bmap**` (Linux) and `slacker` (Windows).

Even when you use sophisticated tools to overwrite the media, traces of the original data may remain as less perceptible magnetic fields. This is like a ghost image that can remain on some older TV and computer monitors if the same data is displayed for long periods of time. Forensics experts and attackers have tools they can use to retrieve this data even after it has been supposedly overwritten. One way to remove data remanence is with a degausser. However, they are only effective on magnetic media. Degaussing SSDs won't remove data (SSDs use integrated circuitry instead of magnetic flux on spinning platters).

Some SSDs include built-in erase commands to sanitize the entire disk, but unfortunately, these weren't effective on some SSDs from different manufacturers. The U.S. National Security Agency (NSA) requires the destruction of SSDs using an approved disintegrator. Approved disintegrators shred the SSDs to a size of 2 millimeters (mm) or smaller.

* 1. Common Data Destruction Methods
     1. Erasing: In most cases, the deletion or removal process removes only the directory or catalog link to the data. The actual data remains on the drive.
     2. Clearing (or Overwriting): a process of preparing media for reuse and ensuring that the cleared data cannot be recovered using traditional recovery tools
     3. Purging: a more intense form of clearing. It provides a level of assurance that the original data is not recoverable using any known methods. Even though purging is intended to remove all data remnants, it isn't always trusted. For example, the U.S. government doesn't consider any purging method acceptable to purge top secret data. Some organizations donate or sell used computer equipment rather than attempting to purge it. They often remove and destroy storage devices that hold sensitive data instead.
     4. Degaussing: creates a strong magnetic field that erases data on some media in a process called degaussing. We don't recommend it. Degaussing a hard disk will normally destroy the electronics used to access the data. Additionally, someone could open the drive in a clean room and install the platters on a different drive to read the data. Degaussing doesn't affect optical CDs, DVDs, or SSDs.
     5. Destruction: ensure that the media cannot be reused or repaired and that data cannot be extracted from the destroyed media. Methods of destruction include incineration, crushing, shredding, disintegration, and dissolving using caustic or acidic chemicals. You can remove the platters in highly classified disk drives and destroy them separately.

Declassification involves any process that purges media or a system in preparation for reuse in an unclassified environment. Often, the efforts required to securely declassify media are significantly greater than the cost of new media for a less secure environment. **Instead** of taking the risk, many organizations choose not to declassify any media and instead destroy it when it is no longer needed.

* 1. Cryptographic Erasure (or cryptoshredding)

If data is encrypted on a device, organizations can destroy both the encryption key and decryption key. You should use another method to overwrite the data. If the original encryption isn't strong, someone may be able to decrypt it without the key. Additionally, there are often backups of cryptographic keys, and if someone discovers a backup key, they can still access the data. When using cloud storage, cryptoshredding may be the only measure for secure deletion.

1. Ensuring Appropriate Data and Asset Retention

Chapter 3, "Business Continuity Planning," covers a vital records program, which can be referenced to identify records to retain.

Records retention involves retaining and maintaining important information as long as it i needed and destroying it when it is no longer needed. Some laws and regulations (security policy or data policy) dictate the length of time that an organization should retain data. It must be identified by organizations even in the absence of external requirements.

As an example, many organizations require the retention of all audit logs for a specific amount of time. These audit logs allow the organization to reconstruct the details of past security incidents. When an organization doesn't have a retention policy, administrators may delete valuable data earlier than management expects them to or attempt to keep data indefinitely. The longer an organization retains data, the more it costs in terms of media, locations to store it, and personnel to protect it.

Retention Policies can reduce liabilities.

1. Data Protection Methods
2. Encryption is a primary methods (discussed in the "Understanding Data States").
3. Digital Rights Management

Here are some methods associated with DRM solutions:

1. DRM License: A license grants access to a product and defines the terms of use.
2. Persistent Online Authentication: Persistent online authentication (also known as always-on DRM) requires a system to be connected with the internet to use a product.
3. Continuous Audit Trail: tracks all use of a copyrighted product. It can detect abuse when combined with persistence such as concurrent use of a product simultaneously but in two geographically different locations.
4. Automatic Expiration: Many products are sold on a subscription basis.

Digital watermarks are sometimes placed within audio or video files using steganography. They don't prevent copying but can be used to detect the unauthorized copying of a file. They can also be used for copyright enforcement and prosecution. Similarly, metadata is sometimes placed into files to identify the buyer.

People against DRM claim it isn't effective against people that want to bypass it but instead complicates the usage for legitimate users.

1. Cloud Access Security Broker (CASB)

A CASB is software placed logically between users and cloud-based resources. It can be on-premises or within the cloud. It monitors all activity and enforces administrator-defined security policies. CASB can also log all access, monitor activity, and send alerts on suspicious activity. In general, any security controls that an organization has created internally can be replicated to a CASB (including any DLP functions implemented by an organization). CASB solutions can detect shadow IT (the use of IT resources without the approval or acknowledgement of the IT department) by collecting and analyzing logs from network firewalls and web proxies. Chapter 16, “Managing Security Operations,” covers other cloud topics.

1. Pseudonymization

Pseudonymization refers to the process of using pseudonyms to represent other data. When pseudonymization is performed effectively, it can result in less stringent requirements that would otherwise apply under the EU GDPR, covered in Chapter 4. As an example, instead of including personal information such as the patient’s name, address, and phone number, it could just refer to the patient as Patient 23456 in the medical record. The doctor’s office still needs this personal information, and it could be held in another database linking it to the patient pseudonym (Patient 23456).

The GDPR refers to pseudonymization as replacing data with artificial identifiers.

1. Tokenization

In the past, credit card data has been intercepted and stolen at the POS system.

1. Anonymization

Anonymization is the process of removing all relevant data so that it is theoretically impossible to identify the original subject or person.

Randomized masking can be an effective method of anonymizing data. Masking swaps data in individual data columns so that records no longer represent the actual data. However, the data still maintains aggregate values that can be used for other purposes, such as scientific purposes.

1. Understanding Data Roles

Different documentation refers to these roles a little differently. Some of the terms you may see match the terminology used in some NIST documents, and other terms match some of the terminology used in the EU GDPR.

* 1. Data Owners (or Organizational Owner)

They have ultimate organizational responsibility for data. The owner can be CEO or a department head (DH).

NIST SP 800-18 Rev. 1, “Guide for Developing Security Plans for Federal Information Systems,” outlines the following responsibilities for the **information owner** (data owner in this case):

* + 1. Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior)
    2. Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides
    3. Decides who has access to the information system and with what types of privileges or access rights
    4. Assists in the identification and assessment of the common security controls where the information resides

NIST SP 800-18 frequently uses the phrase “rules of behavior,” which is effectively the same as an acceptable use policy (AUP). Both outline the responsibilities and expected behavior of individuals and state the consequences of not complying with the rules or AUP. Additionally, individuals are required to periodically acknowledge that they have read, understand, and agree to abide by the rules or AUP (with online electronic digital signature if necessary).

* 1. Asset Owners

The asset own (or system owner) is the person who owns the asset or system that processes sensitive data. NIST SP 800-18 outlines the following responsibilities for the system owner:

* + 1. Develops a system security plan in coordination with information owners, the system administrator, and functional end users
    2. Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements
    3. Ensures that system users and support personnel receive appropriate security training, such as instruction on rules of behavior (or an AUP)
    4. Updates the system security plan whenever a significant change occurs
    5. Assists in the identification, implementation, and assessment of the common security controls.

The system owner is typically the same person as the data owner, but it can sometimes be someone else, such as a different department head (DH). As an example, consider a web server used for ecommerce that interacts with a back-end database server. A software development department might perform database development and database administration for the database and the database server, but the IT department maintains the web server. In this case, the software development DH is the system owner for the database server, and the IT DH is the system owner for the web server. However, if software developers work within the IT department, the IT DH would be the system owner for both systems.

The system owner is responsible for ensuring that data processed on the system remains secure. This includes identifying the highest level of data that the system processes. The system owner then ensures that the system is labeled accurately and that appropriate security controls are in place to protect the data. System owners interact with data owners to ensure that the data is protected while at rest on the system, in transit between systems, and in use by applications operating on the system.

System and data owners are senior personnel within an organization. As a result, management teams typically include system and data owners. This is especially useful when a system has one owner for the system and another owner for the data.

* 1. Business/Mission Owners

The business/mission owner role is viewed differently in different organizations. NIST SP 800-18 refers to the business/mission owner as a **program manager** or an **information system owner**. As such, the responsibilities of the business/mission owner can overlap with the responsibilities of the system owner or be the same role.

Business owners might own processes that use systems managed by other entities. As an example, the sales department could be the business owner, but the IT department and the software development department could be the system owners for systems used in sales processes. Even though the sales department doesn’t own these systems, it does own the **business processes** that generate sales using these systems, in which business owners have to make sure it brings value to the organization.

Compare this with IT departments. If there are any successful attacks or data breaches, the fault is likely to fall on them. IT departments often recommend security controls or systems that don’t add immediate value to the organization but reduce overall risks. The business owner is responsible for evaluating these recommendations and may decide that the potential loss related to the risks they eliminate is less than the loss of revenue they’ll cause. The IT department doesn’t generate revenue. Instead, it is a cost center generating costs. In contrast, the business side generates revenue as a profit center. Costs generated by the IT department may reduce risks, but they eat up profits generated by the business side.

* 1. Data Processors and Data Controllers

Generically, a data processor is any system used to process data. However, in the context of the GDPR, **data processor** has a more specific meaning: “a natural or legal person, public authority, agency, or other body, which processes personal data solely on behalf of the data controllers.” In this context, the **data controller** is the person or entity that controls the processing of the data: they decide what, why, and how to process these data.

As an example, a company that collects personal information on employees for payroll is a data controller. If they pass this information to a third-party company to process payroll, the payroll company is the data processor. In this example, the payroll company must not use the data for anything other than process payroll at the direction of the data controller.

The GDPR restricts data transfers to countries outside the EU. Companies (may face fines of up to 4% of their global revenue). Unfortunately, it is filled with legalese, presenting many challenges for organizations. As an example, clause 107 includes this single sentence statement:

Consequently the transfer of personal data to that third country or international organisation should be prohibited, unless the requirements in this Regulation relating to transfers subject tot appropriate safeguards, including binding corporate rules, and derogations for specific situations are fulfilled.

As a result, many organizations have created dedicated roles, such as a data privacy officer, to oversee the control of data and ensure the organization follows all relevant laws and regulations. The GDPR has mandated the role of a data protection officer for any organization that must comply with the GDPR. The person in this role is responsible for ensuring the organization applies the laws to protect individuals’ private data.

* 1. Data Custodians

Data owners often delegate day-to-day tasks to a data custodian. In practice, personnel within an IT department or system security administrators would typically be the custodians. They might be the same administrators responsible for assigning permissions to data.

* 1. Administrators

Many organizations view anyone with elevated privileges as administrators. For example, help desk employees are granted some elevated privileges to perform their job but aren’t granted full administrative privileges. They are sometimes referred to as administrators. In the context of data roles, a data administrator may be a data custodian or someone in another data role.

* 1. Users and Subjects

A user is any person who accesses data via computing system to accomplish work tasks. You can also think of users as employees or end users (discussed further in Chapter 8, “Principles of Security Models, Design, and Capabilities,” and Chapter 13.

Subjects can be users, programs, processes, services, computers, or anything else that can access a resource.

The GDPR defines a **data subject** as a person who can be identified through an identifier, such as a name, identification number, or other means. If a file includes PII on Sally Smith, Sally Smith is the data subject.

1. Using Security Baselines

Chapter 16 covers imaging in the context of configuration management in more depth. As an introduction, administrators configure a single system with desired settings, capture it as an image, and then deploy the image to other systems. After deploying systems in a secure state, auditing processes periodically check the systems to ensure they remain in a secure state.

NIST SP 800-53 Rev.5, “Security and Privacy Controls for Information Systems and Organizations,” mentions security control baselines and identifies them as a set of minimum security controls defined for an information system. It stresses that a single set of security controls **does not** apply to all situations.

NIST SP 800-53B, “Control Baselines for Information Systems and Organizations,” includes a comprehensive list of security controls and has identified many of them to include in various baselines (four baselines based on the potential impact to an organization’s mission if there is a loss of confidentiality, integrity, or availability of a system):

* 1. Low-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a low impact on the organization’s mission.
  2. Moderate-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a moderate impact on the organization’s mission.
  3. High-Impact Baseline Controls in this baseline are recommended if a loss of confidentiality, integrity, or availability will have a high impact on the organization’s mission.
  4. Privacy Control Baseline This baseline provides an initial baseline for any systems that process PII. Organizations may combine this baseline with one of the other baselines.

You would try to predict the impact of the compromise on the confidentiality, integrity, or availability of the system and any data it holds. If the impact is high, you would consider adding all the controls listed as high-impact in addition to the low-impact and moderate-impact controls. If the compromise would cause privacy data to be compromised, you would consider adding the security controls identified as privacy control baseline items to your baseline.

1. Comparing Tailoring and Scoping

**Tailoring** refers to modifying the list of security controls within a baseline to align with the organization’s mission. NIST SP 800-53B formally defines it as “part of an organization-wide risk management process that includes framing, assessing, responding to, and monitoring information security and privacy risks” and indicates it includes the following activities:

- Identifying and designating common controls

- Applying scoping considerations

- Selecting compensating controls

- Assigning control values

A selected baseline may not include commonly implemented controls.

Imagine that a data center includes video cameras covering the external entry, the internal exit, and every row of servers, but the baseline only recommends a video camera cover the external entry. During the tailoring process, personnel will evaluate these extra cameras and determine if they are needed. They may decide to remove some to save costs or keep them.

An organization might decide that a set of baseline controls applies perfectly to computers in their central location, but some controls aren’t appropriate or feasible in a remote office location. As an example, imagine the account lockout policy is set to lock out users if they enter an incorrect password five times. In this example, the control value is 5, but the tailoring process may change it to 3.

**Scoping** (part of the tailoring process) processes eliminate controls that are recommended in a baseline. For example, if a system doesn’t allow any two people to log on to it simultaneously, there’s no need to apply a concurrent session control.

1. Standards Selection

Organizations need to ensure that the controls comply with external security standards. As an example, the PCI DSS defines requirements that organizations processing credit card transactions must follow. Similarly, organizations that collect or process data belonging to EU citizens must abide by the requirements in the GDPR.

Chapter 16: Managing Security Operations-Provision Resources Securely

An important consideration when provisioning resources securely is asset management. Chapter 13, “Managing Identity and Authentication,” covers provisioning and deprovisioning for accounts as part of the identity and access provisioning lifecycle. This section focuses on resources such as hardware and software assets.

1. Information and Asset Ownership

Data owners typically delegate data protection tasks to others in the organization. For example, employees in the data custodian security role typically perform daily tasks such as implementing access controls, performing backups, and managing data storage.

1. Asset management

**Tangible assets** include hardware and software assets owned by the company. **Intangible assets** include patents, copyrights, a company’s reputation, and other assets representing potential revenue.

Many organizations use an automated configuration management system (CMS) to help with hardware asset management. The primary purpose of a CMS is configuration management, discussed later in this chapter. The CMS needs to connect to hardware systems when checking configuration. The **CMS** needs to connect to hardware systems when checking configuration settings. While doing so, it verifies that the system is still in the network and turned on.

* 1. Hardware Asset Inventories

Hardware assets are IT resources such as computers, servers, routers, switches, and peripherals. Many organizations use databases and inventory applications to perform inventories and track hardware assets through the entire equipment lifecycle. For example, bar-code systems are available that can print bar codes to place on equipment. The bar-code database includes relevant details on the hardware, such as the model, serial number, and location. When the hardware is purchased, it is bar-coded before it is deployed. On a regular basis, personnel scan all of the bar codes with a bar-code reader to verify that the organization still controls the hardware.

A similar method uses radio frequency identification (RFID) tags. These tags transmit information to RFID readers. Personnel place the RFID tags on the equipment and use the RFID readers to inventory the equipment. RFID tags and readers are more expensive than bar codes and bar-code readers. However, RFID methods significanty reduce the time needed to perform an inventory.

When equipment is at the end of its lifetime, it’s easy for individuals to lose sight of the data that it contains, so using checklists to sanitize the system is often valuable. NIST 800-88r1 and Chapter 5 have more information on procedures to sanitize drives.

Portable media, such as USB drives, holding sensitive data is also managed as an asset.

* 1. Software Asset Inventories

Software assets are operating systems and applications. Organizations pay for software, and license keys are routinely used to activate the software. The activation process often requires contracting a licensing server over the internet to prevent piracy. If the license keys are leaked outside the organization, it can invalidate the organization’s use. It’s also important to monitor **license compliance** to avoid legal issues.

For example, an organization could purchase a license key for five software product installations but only install and activate one instance immediately. If the key is stolen and installed on four systems outside the organization, those activations will succeed. When the organization tries to install the application on internal systems, the activation will fail. Any type of license key is highly valuable to an organization and should be protected.

Software licensing also refers to ensuring that systems do not have unauthorized software installed. Many tools are available that can inspect systems remotely to detect the system’s details. This allows them to identify unauthorized software running on systems, and helps an organization ensure that it complies with software licensing rules.

* 1. Intangible Inventories

These are intellectual assets (such as intellectual property, patents, trademarks, a company’s reputation, and copyrights).

The **senior management** team is typically the owner of these assets.

As an example, imaging a company sells a product based on a patent. The revenue from these sales can be used to assign a value to the patent. Patents in the United States are valid for 20 years, so this time frame can also be used when calculating the value. Failing to pay these fees can result in a loss of the patent, stressing the importance of tracking patents.

Large organizations report the value of intangible assets on their balance sheets using generally accepted accounting principles (GAAP). This helps them review their intangible assets at least annually.

Domain 3:

1. Research, implement and manage engineering processes using secure design principles
   1. Threat Modeling

Threat Modeling isn’t meant to be a single event. Instead, it’s meant to be initiated early in the design process of a system and continue throughout its lifecycle. For example, Microsoft uses a Security Development Lifecycle (SDL) with the motto of “Secure by Design, Secure by Default, Secure in Deployment and Communication” (known as SD3+C). It has two goals in mind with this processes: reducing the number of security-related design & coding defects and the severity of any remaining defects.

**Defensive** approach: predicting threats and designing in specific defenses during the coding and crafting process.

**Proactive** approach: integrated security solutions are more cost-effective and more successful than those shoehorned in later

**Adversarial** approach (or threat hunting or **reactive** approach): takes place after a product has been created and deployed. This deployment could be in a test or laboratory environment or to the general marketplace. This technique of threat hunting is the core concept behind ethical hacking, penetration testing, source code review, and fuzz testing. This usually results in less effective security improvements (over defensive threat modeling) at the cost of potentially reducing functionality and user-friendliness.

Identifying threats:

* + 1. Focused on Assets
    2. Focused on Attackers
    3. Focused on Software

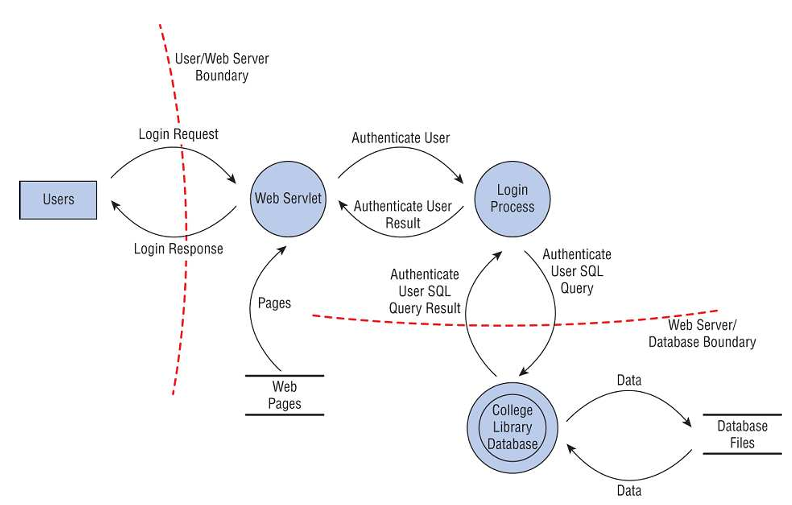
Microsoft developed a threat categorization scheme known as the STRIDE threat model: Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service, and Elevation of privilege.

Process for Attack Simulation and Threat Analysis (PASTA) is a seven-stage threat modeling methodology. It’s a risk-centric approach that aims at selecting or developing countermeasures in relation the value of the assets to be protected.

1. Definition of the Objectives (DO) for the Analysis of Risks
2. Definition of the Technical Scope (DTS)
3. Application Decomposition and Analysis (ADA)
4. Threat Analysis (TA)
5. Weakness and Vulnerability Analysis (WVA)
6. Attack Modeling & Simulation (AMS)
7. Risk Analysis & Management (RAM)

Visual, Agile, and Simple Threat (VAST) is a threat modeling concept that integrates threat and risk management into an Agile programming environment on a scalable basis.

Determining and Diagramming Potential Attacks



Performing Reduction Analysis (decomposing the application, system, or environment):

1. Trust Boundaries: Any location where the level of trust or security changes
2. Dataflow paths: The movement of data between locations
3. Input points: Locations where external input is received
4. Privileged operations: Any activity (typically system changes or altering security) that requires greater privileges than of a standard user account or process.

Prioritization and Response: DREAD ranking system: damage portential, reporducibility, exploitability, affected users, and discoverability.

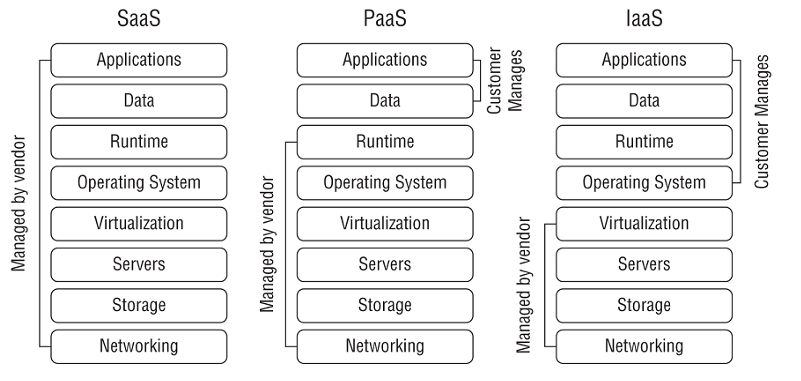
Supply chain risk management (SCRM) is the means to ensure that all of the vendors or links in the supply chain are reliable, trustworthy, reputable organizations that disclose their practices and security requirements to their business partners.

The security requirements for new hardware, software, or services should always meet or exceed the security expected in the final product. This often requires a detailed review of SLAs, contracts, and actual performance. When a supply chain component provider is crafting software or providing a service (such as a cloud provider), then a service-level requirement (SLR) may need to be defined. An SLR is a statement of the expectations of service and performance from the product or service of a vendor. Often, an SLR is provided by the customer/client prior to the establishment of the SLA (which should incorporate the elements of the SLR if the vendor expects the customer to sign the agreement).

The Principle of Least Privilege: states that subjects are granted only the privileges necessary to perform assigned work tasks and no more. Limiting and controlling privileges based on this concept protects confidentiality and data integrity. If users can modify only those data files that their work tasks require them to modify, it protects other files’ integrity in the environment. However, the least privilege principle relies on the assumption that all users have a well-defined job description that peronnel understand. Without a specific job description, it’s not possible to know what privileges users need.

Separation of Duties (SoD) and responsibilities:

1. Two-Person control (two-man rule): requires the approval of two individuals for critical tasks. **Split knowledge** combines the concepts of separation of duties and two-person control into a single solution.
2. Job Rotation: act as a deterrent and a detection machanism. If employees choose to take part in fraudulent activities so anyway, individuals taking over the job responsibilities later are likely to discover the fraud.
3. Mandatory vacations: This provides a form of peer review and helps detect fraud and collusion.
   1. Shared responsibility: indicates that organizations don’t operate in isolation.
      1. Everyone in an organization has some level or security responsibility. It’s the job of the CISO and security team to establish security and maintain it. It’s the job of the regular employees to perform their tasks within the confines of security. It’s the job of the auditor to monitor the environment for violations.
      2. Organizations are responsible to their stakeholders to make good security decisions in order to sustain the organization.
      3. When working with third parties, especially with cloud providers, each entity needs to understand their portion of the shared responsibility of performing work operations and maintaining security (discussed in Chapter 16)
      4. Responsibly disclose new vulnerabilities and threats to the proper vendor or to an **information sharing center** (threat intelligence source or service). **Automated indicator sharing** (AIS) facilitate free exchange of indicators of compromise (**IoCs**) and other cyberthreat information between the U.S. federal government and the private sector. It makes full use of Structured Threat Information eXpression (**STIX**) and Trusted Automated eXchange of Intelligence Information (**TAXII**) to share threat indicators (IoCs). AIS is managed by the National Cybersecurity and Communications Integration Center (NCCIC).
4. Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements.
   1. Shared Responsibility with Cloud service Models



* + 1. Software as a Service (SaaS): SaaS models provide fully functional applications typically accessible via web browser. For example, Gmail is an SaaS application. The vendor (Google in this example) is responsible for all maintenance of the SaaS services.
    2. Platform as a Service (Paas): PaaS models provide consumers with a computing platform, including hardware, operating systems, and a runtime environment (including programming languages, libraries, services, and other tools supported by the vendor. Customers deploy applications that they’ve created or acquired, manage their applications, and possibly modify some configuration settings on the host. However, the vendor is responsible for maintenance of the host and the underlying cloud infrastructure.
    3. Infrastructure as a Service (IaaS).

NIST SP 800-145, The NIST Definition of Cloud Computing, provides standard definitions for many cloud-based services. NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, provides in-depth details on security issues related to cloud-based computing.

The four cloud deployment models available are as follows:

1. A **public cloud** model includes assets available for any consumers to rent or lease and is hosted by an external CSP.
2. The **private cloud** deployment model is used for cloud-based assets for a single organization. Organizations can create (and also hold responsibility for) and host private clouds using their own on-premises resources. Maintenance requirements are typically split based on the service model (SaaS, PaaS, or IaaS).
3. A **community cloud** deployment model provides cloud-based assets to two or more organizations that have a shared concern, such as similar mission, security requirements, policy, or compliance considerations. Maintenance responsibilities are shared based on who is hosting the assets and the service models.
4. A **hybrid cloud** model includes a combination of two or more clouds that are bound together by a technology that provides data and application portability. Maintenance responsibilities are similar to a community cloud model.
   1. Cryptographic system
      1. Asymmetric Cryptography: RSA (was once patent), Merkle-Hellman Knapsack (proven ineffective when it was broken in 1984), ElGamal (wasn’t patent but has a major disadvantage: the algorithm doubles the size of any message that it encrypts), Elliptic Curve (3,072-bit RSA key is cryptographically equivalent to a 256-bit elliptic curve cryptosystem key)
      2. Symmetric Cryptography: AES…
      3. Hash: Numberous hashing algorithms are not addressed on the exam, but in addition to SHA (cryptanalytic attacks demonstrated that there are weakenesses in the SHA-1 algorithm, and therefore, NIST deprecated SHA-1 and web browsers dropped support for SHA-1 in 2017), MD5, RIPEMD, and HMAC, you should recognize HAVAL. Hash of Variable Length (HAVAL) is a modification of MD5. HAVAL uses 1,024-bit blocks and produces hash values of 128, 160, 192, 224, and 256 bits.
         1. SHA-1 produces a 160-bit message digest by processing a message in 512-bit block size.
         2. SHA-2 has 4 variant: SHA-256 and SHA-224 produce a 256-bit and 224-bit message, respectively, by processing a message in 512-bit block size. SHA-512 and SHA-384 produce a 512-bit and 384-bit message, respectively, by processing a message in 1024-bit block size.
         3. In 2015, the federal government announced the release of the Keccak algorithm as the SHA-3 standard, which is slower than and provides the same level of security as SHA-2.
         4. MD2 (secure hash function for 8-bit processors), MD4 (for 32-bit processors), and MD5 (use 4 distinct rounds of computation and has the same padding requirements as MD4-the message length must be 64 bits less than a multiple of 512 bits) are subjected to cryptanalytic attacks.
         5. RIPEMD (128-bit digest), RIPEMD-128, and RIPEMD-160 (most commonly used of the RIPEMD variants and produces a 160-bit hash value) are used in Bitcoin cryptocurrency implementations. RIPEMD-256 and RIPEMD-320 have the same level of security as RIPEMD-128 and RIPEMD-160, respectively.

Digital Signatures has two distinct goals: enforcing non-repudiation and integrity. Additionally, software vendors often use digital signature technology to authenticate code distributions that you download from the internet, such as applets and software patches. Meanwhile, the hashed message authentication code (HMAC) algorithm implements a partial digital signature-it guarantees the integrity of a message during transmission, but it doesn’t provide for non-repudiation.

Digital Signature **Standard**: The NIST specifies the digital signature algorithms acceptable for federal government use in Federal Information Processing Standard (FIPS) 186-4, also known as the Digital Signature Standard (DSS). This document specifies that all federall y approved digital signature algorithms must use the SHA-3 hashing functions. There are 3 currently approved standard encryption algorithms:

- The DSA as specified in FIPS 186-4. This algorithm is a variant of an algorithm developed by Dr. Taher Elgamal.

- The RSA algorithm, as specified in ANSI X9.31

- The Elliptic Curve DSA (ECDSA), as specified in ANSI X9.62.

- The FIPS 186-5 remains in draft form. The draft proposal removes DSA as an approved algorithm, retains RSA and ECDSA, and adds the Edwards-Curve DSA (EdDSA) to DSS.

* 1. PKI
     1. Certificates:

Before the TLS handshake: You, as the server, need to request and receive a certificate from the CA by submitting a CSR. Digital certificates (signed by a trusted CA) that conform to X.509 contain the following data:

* + - 1. Version of X.509 to which the certificate conforms.
      2. Serial number (from the certificate creator)
      3. Signature algorithm identifier (specifies the technique used by the certificate authority to digitally sign the contents of the certificate)
      4. Issuer name (identification of the certificate authority that issued the certificate)
      5. Validity period (specifies the dates and times-a starting data and time and an expiration data and time-during which the certificate is valid)
      6. Subject’s name (contains the common name [CN] of the certificate as well as the distinguished name [DN] of the entity that owns the public key contained in the certificate)
      7. Subject’s public key (the meat of the certificate-the actual public key the certificate owner used to set up secure communications).

Certificates may be issued for a variety of purposes. These include providing assurance for the public keys of

- Computers/machines

- Individual users

- Email addresses

- Developers (code-signing certificates).

Some major CAs: Symantec, IdenTrust, AWS, GlobalSign, Comodo, Certum, GoDaddy, DigiCert, Secom, Entrust, Actalis, Trustwave.

If you configure your browser to trust a CA, it will automatically trust all of the digital certificates issued by that CA. Browser developers pre-configure browsers to trust the major CAs to avoid placing this burden on users. “Let’s Encrypt!” is a well-known CA because they offer free certficates in an effort to encourage the use of encryption.

Registration authorities (RAs) assist CAs with the burden of verifying users’ identities prior to issuing digital certificates.

CA must carefully protect their own private keys to preserve their trust relationships. They often use an **offline** CA to protect their **root certificate**, the top-level certificate for their entire PKI. This offline CA is disconneted from networks and powered down until it is needed.

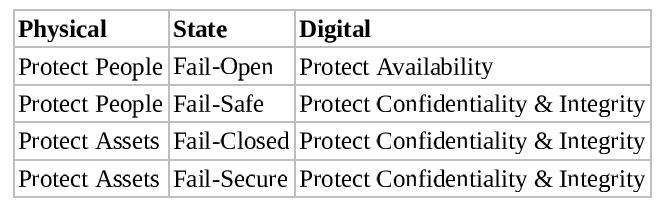
In the CA trust model, the use of a series of intermediate CAs is known as **certificate chaining**. CAs don’t need to be third-party service providers. Many organizations operate internal CAs that provide self-signed certificates for use inside an organization. These certificates won’t be trusted by the browsers of external users.

Certificate Lifecycle:

* + 1. Enrollment: The simplest, and most common, certificates are Domain Validation (DV) certificates, where the CA simply verifies that the certificate subject has control of the domain name. Extended Validation (EV) certificates provide a higher level of assurance and the CA takes steps to verify that the certificate owner is a legitimate business before issuing the certificate.
    2. Verification: when you receive a digital certificate from someone (typically the start of the TLS handshake) with whom you want to communicate, you verify the certificate by checking the CA’s digital signature using the CA’s public key. Finally, you must check and ensure that the certificate was not revoked using a certificate revocation list (**CRL**) or the Online Certificate Status Protocol (**OCSP**). In 2017, Google announced that the Chrome browser would no longer trust Symantec certificates. A series of seemingly small lapses in procedure can decimate a CA’s business.
    3. Revocation: It may occur for one of the following reasons: the certificate was compromised, the certificate was erroneously issued, the details of the certificate changed, and the security association changed. The primary issue with OCSP is that it places a significant burden on the OCSP servers operated by CAs. **Certificate stapling** is an extension to the OCSP that relieves some of the burden placed on certificate authorities by the original protocol. In certificate stapling, the web server contacts the OCSP server itself and receives a signed and timestamped response from the OCSP server, which it then attaches, or staples, to the digital certificate. Then, when a user requests a secure web connection, the web server sends the certificate with the stapled OCSP response to the user. It’s common to have stapled certificates with a validity period of 24 hours.

Certificate Formats:

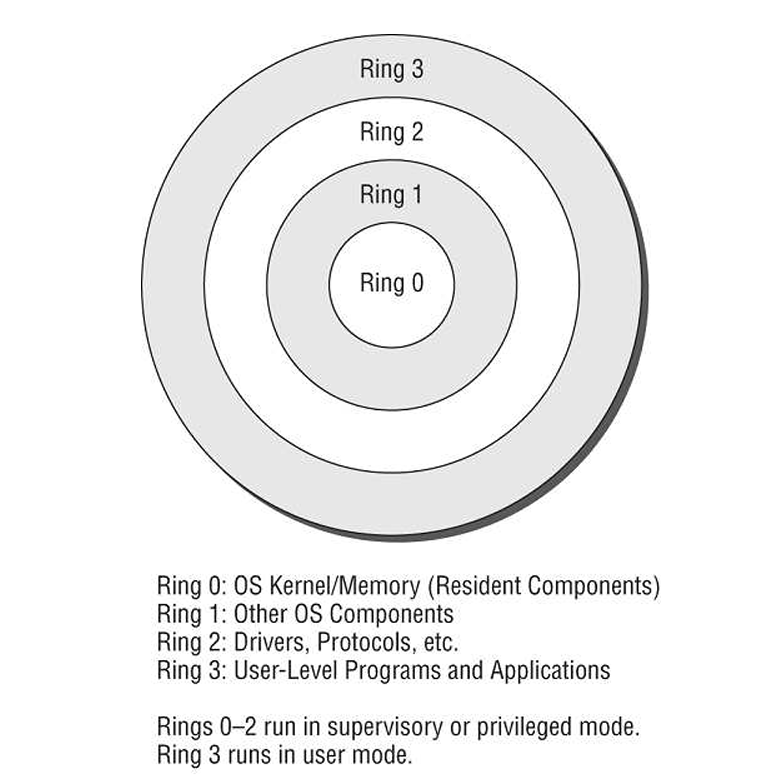
* + - 1. The most common binary format is the Distinguished Encoding Rules (DER) format, which has .der, .crt, or .cer extension.
      2. The Privacy Enhanced Mail (PEM) certificate format is an ASCII text version of the DER format. PEM certificates are normally stored in files with the .pem or .crt extension
      3. The Personal Information Exchange (PFX) format is commonly used by Windows systems. PFX certificates may be stored in binary form, using either .pdx or .p12 file extensions. Windows systems also use P7B certificates, which are stored in ASCII text format.
  1. Asymmetric Key Management
     1. “Security through obscurity” (**STO**, protecting data by hiding the details) is not an appropriate approach. Be wary of systems that use a “**black-box**” (focusing only inputs and outputs instead of internal) approach and maintain that the secrecy of their algorithm is critical to the integrity of the cryptosystem.
     2. If you don’t have a formal policy that you must follow, select an appropriate interval based on the frequency with which you use your key. You might want to change your key pair every few months, if practical.
     3. Back up your key! You may want to either create your own backup or use a key escrow service that aintains the backup for you. Talking about backing up the keys, cryptoshredding is the only way to destroy cloud storage.
     4. Hardware security modules (**HSMs**) also provide an effective way to manage encryption keys. These hardware devices store and manage encryption keys in a secure manner that prevents humans from ever needing to work directly with the keys. Many of them are also capable of improving the efficiency of cryptographic operations, in a process known as **hardware acceleration**. HSMs range in scope and complexity from very simple devices, such as the YubiKey (storing encrypted keys on a USB drive for personal use). HSMs include tamper-resistance mechanisms to prevent someone who gains physical access to the device form accessing the cryptographic material it maintains. There’s also could-based HSMs that provide secure key management for IaaS services.
  2. Hybrid Cryptography: combines symmetric and asymmetric cryptography to achieve the key distribution benefits of asymmetric cryptosystems with the speed of symmetric algorithms. These approaches work by setting up an initial connection between two communicating entities using asymmetric cryptography. That connection is used for only one purpose: the exchange of a randomly generated shared secrety key, known as an **ephemeral key**. The two parties then exchange whatever data they wish using the shared secret key with a symmetric algorithm.
  3. Applied Cryptography
     1. Portable devices: Current versions of popular operating systems now include disk encryption capabilities that make it easy to apply and manage encryption on portable devices. For example, Microsoft Windows includes the **BitLocker** and Encrypting File System (**EFS**) technologies, macOS includes **FileVault** encryption, and the **VeraCrypt** open source package allows the encryption of disks on Linux, Windows, and Mac systems.
     2. The Trusted Platform Module (**TPM**) is a chip that resides on the motherboard of the device. The TPM serves a number of purposes, including the storage and management of keys used for full-disk encryption (**FDE**) solutions. The TPM provides the operating system with access to the keys only if the user successfully authenticates, preventing someone from removing the drive to place it into another device. Don’t forget about smartphones when developing your portable device encryption policy. Most major smartphone and tablet platforms include enterprise-level functionality that supports encryption of data stored on the phone
     3. Email: If you need confidentiality when sending an email message, encrypt the message. If your message must maintain integrity, you must hash the message. If your message needs authentication, integrity, and/or non-repudiation, you should digitally sign the message. If your message requires confidentiality, integrity, origin authentication, and non-repudiation, you should encrypt and digitally sign the message. You’ll find more coverage of email security topics in Chapter 12, “Secure Communications and Network Attacks.”
        1. Phil Zimmerman’s Pretty Good Privacy (**PGP**) secure email system appeared on the computer security scene in 1991. It combines the CA hierarchy described earlier in this chapter with the “web of trust” concept-that is, you must become trusted by one or more PGP users to begin using the system. The most difficult obstruction was the U.S. government export regulations, which treated encryption technology as munitions and prohibited the distribution of encryption technology outside the US. Fortunately, this restriction has since been repealed. PGP is availabe in two versions: the commercial product that is now sold by Symantec and an open source variant called OpenPGP. These products allow for the use of modern encryption algorithms, hash functions, and signature standards within the PGP framework.
        2. S/MIME: The Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol uses the RSA encryption algorithm and has received the back of major industry players, including **RSA Security**. It has already been incorporated in **Microsoft Outlook and Office 265, Apple Mail,** and **Google G Suite Enterprise edition**. S/MINE relies on the use of X.509 certificates.
     4. Web Applications: Over the years, security researchers discovered a number of critical flaws in the SSL protocol that render it insecure for use today. However, SSL serves as the technical foundation for its successor, TLS, which remains widely used today. Cipher suites are usually expressed in long strings that combine each of the four combinations of encryption algorithms (for example, TLS\_DH\_RSA\_WITH\_AES\_256\_CBC\_SHA384). You may also see cipher suites that use DHE or ECDHE. The “E” indicates the algorithm uses different, ephemeral keys for each communication to provide forward secrecy and reduce the likelihood of key compromise. The “E” versions of these algorithms provide added security, but this comes at the cost of added computational complexity.
     5. Tor and the Dark Web: Tor (formerly known as The Onion Router) provides a mechanism for anonymously routing traffic across the internet using encryption and a set of relay nodes. It relies o a technology known as **perfect forward secrecy**.
     6. Steganography and Watermarking: It’s also possible to embed messages inside larger excerpts of text. Steganography techniques are often used for illegal activities, such as espionage and child pornography. Adding digital watermarks to documents to protect intellectual property is accomplished by means of steganography. If there’s an unauthorized copy of the content, the watermark can be used to detect the copy and trace the offending copy back to the source.
     7. Networking:
        1. Circuit Encryption: Security administrators use two types of encryption techniques to protect data-in-transit: **Link encryption** (creating a secure tunnel between two points using either a hardware solution or a software solution that encrypts all traffic entering one end of the tunnel and decrypts all traffic leaving the other end of the tunnel) and **end-to-end** encryption (TLS and SSH as examples). The critical difference between link and end-to-end encryption is that in link encryption, all the data, including the header, trailer, address, and routing data, is also encrypted. End-to-end moves faster from point to point but is more susceptible to sniffers and eavesdroppers. There are actually two versions of SSH: SSH1 (considered insecure) and SSH2 (dropping support for DES and IDEA but adds support for the DHKE and the ability to run multiple sessions over a single SSH connection). SSH2 provides added protection against MITD attacks, eavesdropping, and IP/DNS spoofing.
        2. IPsec: is a standard architecture set forth by the Internet Engineering Task Force (IETF) for setting up a secure channel to exchange information between two entites. IPsec relies on security associations and there are 2 main components: the Authentication Header (**AH**) and the Encapsulating Security Payload (ESP). ESP also provides some limited authentication, but not to the degree of the AH. Though ESP is sometimes used without AH, it’s rare to see AH used without ESP. IPsec provides 2 discrete modes of operation: **transport** mode (for end-to-end encryption) and **tunnel** mode (for link encryption). You set up an IPsec session by creating a **security association** (SA, representing the communication session and records any configuration and statuts information about the connection). If you want a two-way channel, you need two SAs, one for each direction. Also, if you want to support a bidirectional channel using both AH and ESP, you will need to set up four SAs. Some of IPsec’s greatest strengths come from being able to filter or manage communications on a per-SA basis so that clients or gateways between which security associations exist can be rigorously managed in terms of what kinds of protocols or services can use an IPsec connection. Further details of the IPsec algorithm are provided in Chapter 11.
        3. Emerging applications
           1. Blockchain: MFA needs this. Blockchain technology might also be used to track supply chains, providing consumers with confidence that their produce came from reputable sources.
           2. Lightweight Cryptography: low-latency and power-saving. In cases where resiliency is extremely important, the easiest way to address is for the sender of data to retain a copy until the recipient confirms the successful receipt and decryption of the data.
           3. Homomorphic Encryption
        4. Cryptographic Attacks:
           1. Analytic Attack: is an algebraic manipulation that attempts to reduce the complexity of the algorithm.
           2. Implementation Attack: exploits weaknesses in the implementation of a cryptography system.
           3. Statistical Attack: exploits statistical weaknesses such as floating-point errors and inability to produce truly random numbers.
           4. Brute-Force Attack
           5. Fault Injection Attack: compromise the integrity of a cryptographic device by causing some type of external fault
           6. Side-Channel Attack: computer systems generate characteristic footprints of activity. Side-channel attacks seek to use this information to monitor system activity and retrieve information that is actively being encrypted.
           7. Timing Attack: an example of a side-channel attack where the attacker measures precisely how long cryptographic operations take to complete, gaining information about the cryptographic process that may be used to undermine its security
  4. Secure Design Principles
     1. Closed and Open systems: a **closed system** is designed to work well with a narrow range of other systems, generally all from the same manufacturer. The standards for closed systems are often proprietary and not normally disclosed. Open systems are much easier to integrate with systems from different many facturers that support the same standards or that use compatible APIs. However, **closed source** code is sometimes revealed through either vendor compromise (a breach of ethics and often the law) or through decompiling or disassembly (ethical reverse engineering or systems analysis).
     2. Secure Defaults: “a rigorous condition imposed by some outside agency or force”. Most devices have a default password, which minimizes the costs of support when installing or using the product for the first time. Default settings often make discovery and exploitation of equipment trivial for attackers. It’s always up to the system’s administrator and/or company security staff to alter a product’s settings to comply with the organization’s security policies.
     3. Fail Securely: One such mechanism, which is supported by many languages, is a try..catch statement. The first question to be resolved is whether the system can operate in a fail-soft mode (to allow a system to continue to operate after a component fails). In physical world situations, it can be bank vault, medical lab, or even data center. A fail-secure system prioritizes the physical security of assets over any other consideration. The terms **fail-open** is a synonym to **fail-safe** and **fail-closed** is a synonym of **fail-secure**.



* + 1. “Keep it simple” (or KISS, “keep it stupid simple”): encouragement to avoid overcomplicating the environment, organization, or product design. Similar terms are “Don’t Repeat Yourself” (**DRY**, not repeating the same code in multiple places, which increase the difficulty in changes), **computing minimalism** (a goal of the program evaluation and review technique, **PERT**), **rule of least power**, “**worse is better**” (aka New Jersey Style, fewer functions but maybe more secure), “**you aren’t gonna need it**” (YAGNI, don’t add functions if it’s not necessary).
    2. Zero Trust & Trust but Verify
    3. Privacy by Design (**PbD**): integrate privacy protections into products during the early design phase. The PbD framework is based on seven foundational principles:
       1. Proactive not reactive; preventive not remedial
       2. Privacy as the default
       3. Privacy embedded into design
       4. Full functionality - positive-sum, not zero-sum
       5. End-to-end security - full lifecycle protection
       6. Visibility and transparency
       7. Respect for user privacy

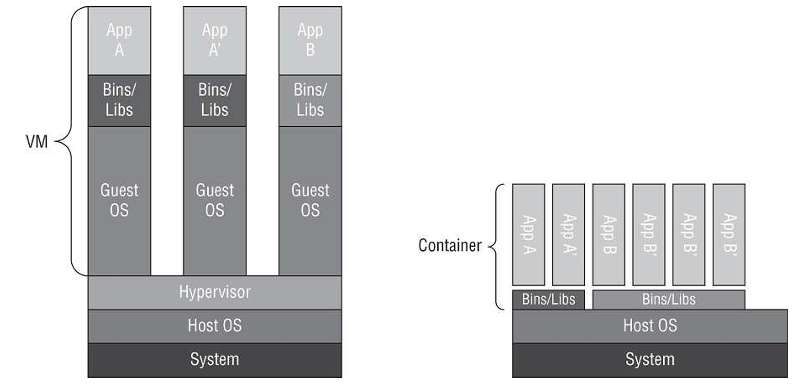
The goal of PbD is to have developers integrate privacy protections into their solutions. It led to the **Global Privacy Standard** (GPS), creating a single set of universal privacy principles (which is integrated in EU’s GDPR).

* + 1. Ensuring CIA: confinement (allowing a process to read from and write to only certain memory locations and resources, or **sandboxing**), bounds (of a process consist of limits set on the memory addresses and resources it can access), isolation (used to protect the operating environment, allowing for a fail-soft environment), access control, trust (typically **trusted system**, where all protection mechanisms work together to process sensitive data for many types of users while maintaining a stable and secure computing environment) and assurance (the degree of confidence in satisfaction of security needs)
  1. Hardware: we all know
  2. Processor: CPU
  3. Execution Types:
     1. Multitasking: handling two or more tasks simultaneously
     2. Multicore: CPU contains two or more independent execution cores. Some chips contain over 10000 cores.
     3. Multiprocessing: using more than 1 processor to complete the execution of a multi-threaded application.
     4. Multiprogramming: similar to multitasking. It involves the pseudo-simultaneous execution of two tasks on a single processor coordinated by the OS to increase operational efficiency.
     5. Multi-threading: mentioned above, it permits multiple concurrent tasks to be performed within a single process.
  4. Protection Mechanisms: The ways in which running computers implement and handle security at runtime may be broadly described as a collection of protection mechanisms, such as protection rings and operational states:
     1. Protection rings: organize code and components in an OS (like applications, utilities, or other code that runs under the OS’s control) into concentric rings. Though the original Multics Implementation allowed up to seven rings (numbered 0 through 6), most modern OSs use a four-ring model (numbered 0 through 3). The part of an OS that always remains resident in memory is called the **kernel**. It occupies ring 0 and can preempt (prevent) code running at any other ring. The remaining parts of the OS occupy ring 1. Ring 2 is also somewhat privileged in that it’s where I/O drivers and system utilities reside; these are able to access peripheral devices, special files, and so forth that applications and other programs cannot themselves access directly. Those applications and programs occupy ring 3 (outermost ring).

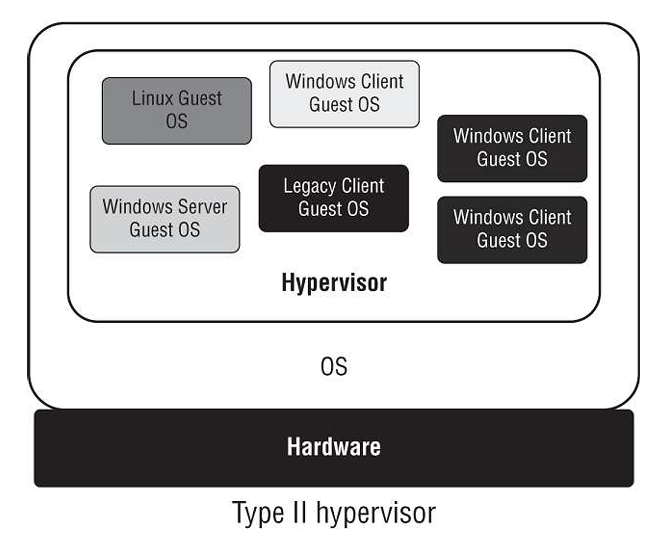


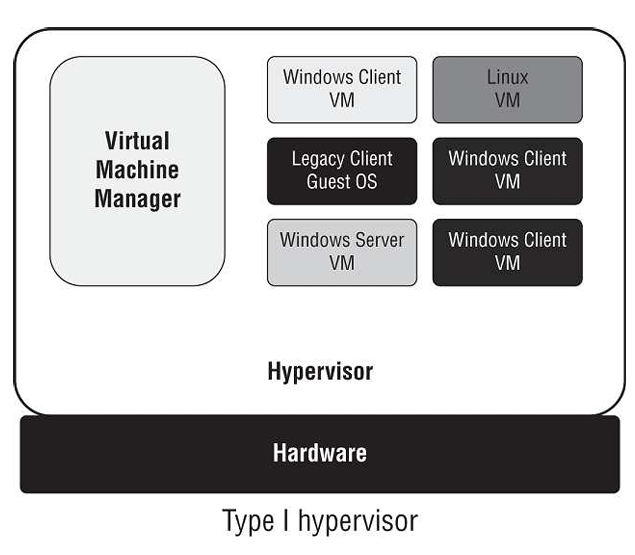
Those processes that run in higher-numbered rings must generally ask a handler or a driver in a lower-numbered ring for services they need (aka **system call**), called **mediated-access model**. In practice, many moderns OSs use only two rings or divisions: one for system-level access (ring 0-2, kernel mode or privileged mode), and on for user-level programs and applications (ring 3, often called user mode).

* + 1. Process states (or operating states): various forms of execution in which a process may run. Where the OS is concerned, it can be in one of two modes at any given moment: operating in a privileged, all-access mode known as **supervisor state** or operating in what’s called the **problem state** associated with user mode where all access requests must be checked against credentials for authorization.
  1. Recording Microphone: can be controlled by MDM/UEM in sensitive areas or meetings
  2. Wi-Fi Direct: new name for the wireless topology of ad hoc or peer-to-peer connections. Recommend use WPA2 or WPA3 in business environments (cuz it has encryption).
  3. Tethering and Hotspots: hotspots devices operate as portable WAPs. It should be barred from use in most organizations cuz they create direct link to the internet without a company’s security restrictions.
  4. Contactless Payment Methods: some are based on NFC, RFID, SMS, or optical camera-based solutions (QR-codes).
  5. SIM Cloning: Physical control must be maintained on mobile devices and an account or service lock established on mobile services with the telco carrier.
  6. Covert Channels:
     1. Covert Timing Channel: conveys information by altering the performance of a system component or modifying a resource’s timing in a predictable manner. Very difficult to detect
     2. Covert Storage Channel: conveys information by writing data to common storage area where another process can read it.
  7. Rootkits: malwre that embeds itself deep within an OS. Notice when system files, such as device drivers and dynamic-link libraries (DLLs), have file size and/or hash value change. File hash tracking can be performed manually by an administrator or automatically by HIDSs (host-based IDS) and system monitoring security tools.
  8. Incremental Attacks:
     1. Data diddlings: attacker gains access to a system and makes small, random, or incremental changes to data during storage, processing, input, output, or transaction.
     2. Salami attack: (myth) systematic whittling at assets in accounts or other records with financial value.
  9. Third-Party Application Stores: Sometimes are blocked to prevent malware.
  10. Industrial Control Systems (ICS): a form of computer-management device that controls industrial processes and machines, also known as **operational technology** (OT). Several forms of ICS are distributed control systems (DCSs), programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA). A DCS focuses on processes and is state driven, whereas SCADA focuses on data-gathering and is event driven. A DCS is used to control processes using a network of sensors, controllers, actuators, and operator terminals and is able to carry out advanced process control techniques. SCADA is suitable for managing systems over large geographic areas. PLC units are effectively single-purpose or focused-purpose digital computers. They are typically deployed for the management and automation of various industrial electromechanical operations.
  11. Grid computing: a form of parallel distributed processing that loosely groups a significant number of processing nodes to work toward a specific processing goal. When a system is otherwise in an idle state, it could join a grid group, download a small portion of work, and being calculations.
  12. Firmware (or microcode): software that is stored in a ROM or an EEPROM. It often drives the basic operation of a computing device.
  13. Large-Scale Parallel Data Systems: a computation system designed to perform numerous calculations simultaneously.
  14. Serverless Architecture: a cloud computing concept where code is managed by the customer and the platform or server is managed by the cloud service provider (CSP). It’s also known as function as a service (**FaaS**). With this, the functions run only when called and then terminate when their operations are completed, thus minimizing costs.
  15. Infrastructure as Code (IaC): is a change in how hardware management is perceived and handled.
  16. Software-defined everything (SDx): a trend of replacing hardware with software using virtualization.
      1. Virtual desktop infrastructure (VDI): hosting desktop/workstation OS virtual machines on central servers that are remotely accessed by the users. It’s also known as VDE (virtual desktop envirnment). Updating the host system doesn’t update the guest OSs. Don’t forget to update hypervisor as well.
      2. VM sprawl occurs when an organization deploys numerous virtual machines without an overarching IT management or security plan in place.
      3. Software-defined visibility (SDV): a framework to automate the processes of network monitoring and response. It provides security and IT management with oversight into all aspects of the company network, both on-premises and in the cloud, with an emphases on defense and efficiency. SDV is another derivative of IaC.
      4. Anything as a Service (XaaS): computing service or capability that can be provided to customers through or over a cloud solution. One area of growth in XaaS is security as a service (SECaaS), also referred to as a managed service provider (MSP) or a mangaed security service provider (MSSP).
      5. Containerization (or OS-virtualization): evolution of the virtualization trend for both internally hosted systems and cloud providers and services.



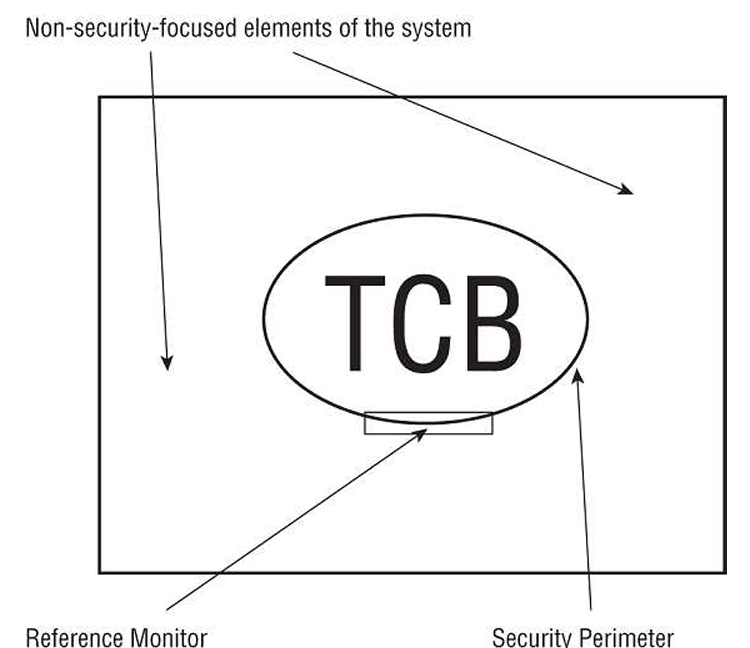
Some deployments claim to eliminate the hypervisor altogether and replace it with a collection of common binaries and libraries for the containers to call upon when needed.



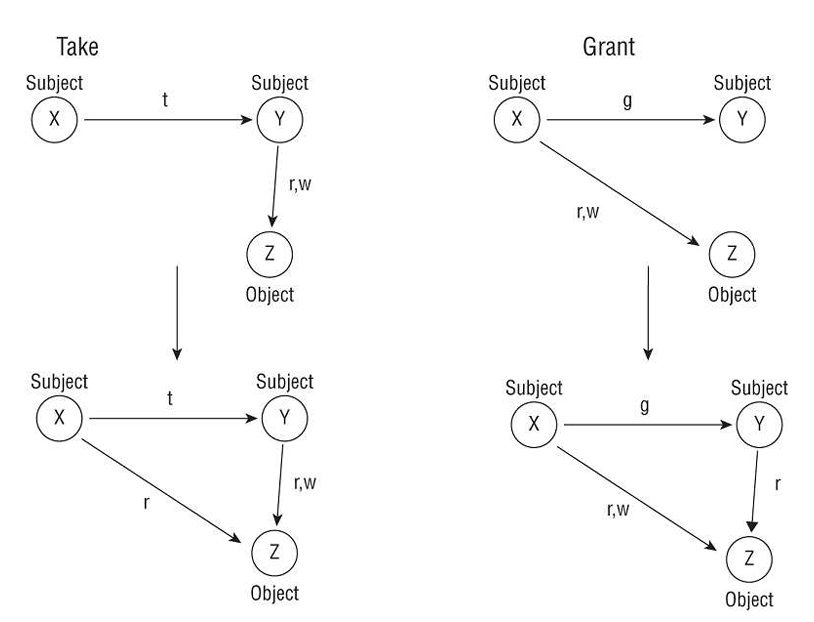


1. Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)

A **capabilities list** maintains a row of security attributes for each controlled object. A subject performs actions or operations within the system while an object contains data or resources that the subject interacts with.



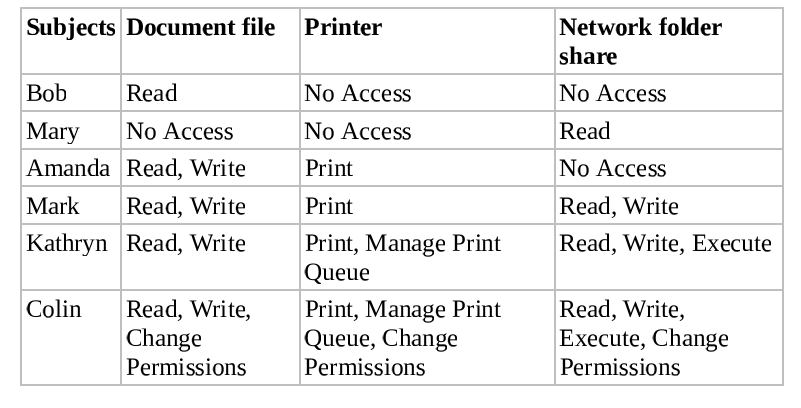
* 1. Trusted Computing Base: a design principle, a combination of hardware, software, and controls that work together to form a trusted base to enforce your security policy. It’s the responsibility of TCP components to ensure that a system behaves properly in all cases and that it adheres to the security policy under all circumstances.
  2. Security Perimeter: an imaginary boundary that separates the TCB from the rest of the system. It may allow for the use of a **trusted shell** (allowing a subject to perform command-line operations without risk to the TCB or the subject).
  3. Reference Monitors and Kernels: a part of the TCB that validates access to every resource prior to granting access requests.
  4. State Machine Model: describes a system that is always secure no matter what state it is in, based on the computer science definition of a **finite state machine** (FSM). An FSM combines an external input with an internal machine state to model all kinds of complex systems, including parsers, decoders, and interpreters. Given an input and a state, an FSM transitions to another state and may create an output. Mathematically, the next state is a function of the current state and the input next state. Likewise, the output is also a function of the input and the current state output. **State transition** occur when accepting input or producing output. All state transitions must be evaluated. If each possible state transition results in another secure state, the system can be called a **secure state machine**.
  5. Information Flow Model: focuses on controlling the flow of information and are based on the state machine model. Not only they deal with the direction of information but also address the type of flow. They prevent unauthorized information flow, often between different levels of security (multilevel models). Information flow can be between subjects and objects at the same or different classification levels. An information flow model allows all authorized information flows, and prevents all unauthorized information flows. Another interesting perspective on the information flow model is that it is used to establish a relationship between two versions or states of the same object when those two versions or states exist at different points in time. Bell-LaPadula Model is an example.
  6. Noninterference Model: is loosely based on the information flow model. Instead, this model is concerned with how the actions of a subject at a higher security level affect the one at a lower security level. This model can be imposed to provide a form of protection against damage caused by malicious programs, such as Trojan horses, backdoors, and rootkits.
  7. Some models that fall into the information flow category build on the notion of inputs and outputs between multiple systems. These are called **composition theories**:
     1. Cascading: Input for one system comes from the out of another system
     2. Feedback: One system provides input to another system, which reciprocates by reversing those roles (so that system A first provides input for system B and then system B provides input to system A).
     3. Hookup: One system sends input to another system but also sends input to external entities.
  8. Take-Grant Model: A subject (X) with the grant right can grant another subject (Y) or another object (Z) any right that subject (X) possesses. Likewise, a subject (X) with the take right can take a right from another subject (Y).



* + 1. Take rule: Allows a subject to take rights over an object
    2. Grant rule: Allows a subject to grant rights to an object
    3. Create rule: Allows a subject to create new rights
    4. Remove rule: Allows a subject to remove rights it has

It is interesting to ponder that the take and grant rules are effectively a copy function. This can be recognized in modern OSes in the process of inheritance, such as subjects inheriting a permission from a group or a file inheriting ACL values from a parent folder.

* 1. Access Control Matrix



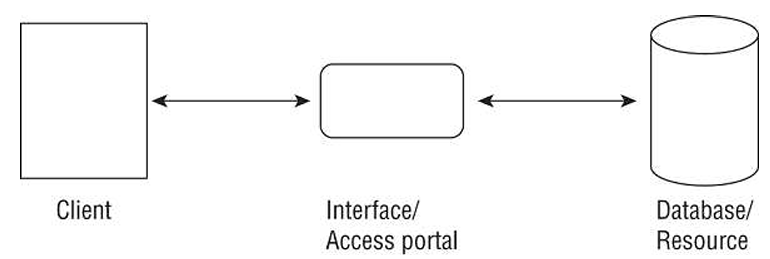
* 1. Bell-LaPadula Model:
     1. The Simple Security Property states that a subject may not read information at a higher sensitivity level (no read-up)
     2. The \* (start) Security Property states that a subject may not write information to an object at a lower sensitivity level (no write-down). This is also known as the Confinement Property.
     3. The Discretionary Security Property states that the system uses an access matrix to enforce discretionary access control.

The Bell-LaPadula model was designed in the 1970s, so it doesn’t support many operations that are common today, such as file sharing and networking. It also assumes secure transitions between security layers and doesn’t address **covert channels** (Chapter 9).

* 1. Biba Model: designed after the Bell-LaPadula model but focuses on integrity:
     1. The Simple Integrity Property states that a subject cannot read an object at a lower integrity level (no read-down).
     2. The \* (star) Integrity Property states that a subject cannot modify an object at a higher integrity level (no write-up).

Biba address 3 integrity issues: prevent modification of objects by unauthorized subjects, prevent unauthorized modification of objects by authorized subjects ,and protect internal and external object consistency. However, critiques of the Biba model reveal a few drawbacks: It addresses only integrity, not confidentiality or availability; It focuses on protecting objects from external threats, assuming that internal threats are handled programmatically; It does not address access control management, and it doesn’t provide a way to assign or change an object’s or subject’s classification level; It doesn’t prevent covert channels.

* 1. Clark-Wilson Model: uses a multifaceted approach to enforcing data integrity. It doesn’t require the use of a lattice structure; it uses a three-part relationship of subject/program/object (or subject/transaction/object, known as triple or an **access control triplet**). Objects can be accessed only through programs. Throughout the use of “well-formed transactions” and “separation of duties”, this model provides an effective means to protect integrity. Well-formed transactions take the form of programs. A subject is able to access objects only by using a program, interface, or access portal. Each program has specific limitations on what it can and cannot do to an object (such as database or other resource). This effectively limits the subject’s capabilities.



Clark-Wilson defines the following items and procedures:

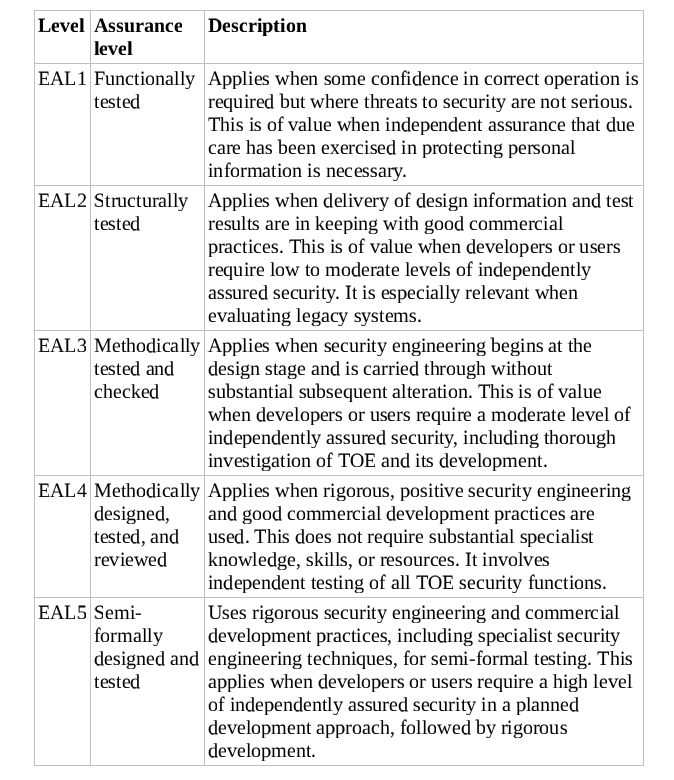
* + 1. A **constrained data item** (CDI) is any data item whose integrity is protected by the security model
    2. An **unconstrained data item** (UDI) is any data item that is not controlled by the security model. Any data that is to be input and hasn’t been validated, or any output.
    3. An **integrity verification procedure** (IVP) is a procedure that scans data items and confirms their integrity.
    4. **Transformation procedures** (TPs) are the only procedures that are allowed to modify a CDI.
  1. Brewer and Nash Model: permit access controls to change dynamically based on a user’s previous activity (a kind of state machine model as well). It’s sometimes known as the Chinese Wall model, ethical wall, or cone of slience
  2. Goguen-Meseguer Model: a less well-known integrity model. It’s said to be the foundation of noninterference conceptual theories. It’s based on predetermining the set or domain (a list) of objects that a subject can access. It’s based on automation theory and domain separation. Thus, subjects are unable to interfere with each other’s activities.
  3. Sutherland Model: another integrity model. It focuses on preventing interference in support of integrity. It’s based on the idea of defining a set of system states, initial states, and state transitions. It’s used to prevent a covert channel from being used to influence the outcome of a process or activity.
  4. Graham-Denning Model: focused on the secure creation and deletion of both subjects and objects. Additionally, securely provide the read, grant, delete, and transfer access right.
  5. Harrison-Ruzzo-Ullman Model (HRU): an extension of Graham-Denning model. The state of access rights under HRU can be expressed in a matrix. It defines the intersection of each row and column with procedures allowed. Additionally, a finite set of commands (or primitives) controls how the matrix can be modified by authorized subjects

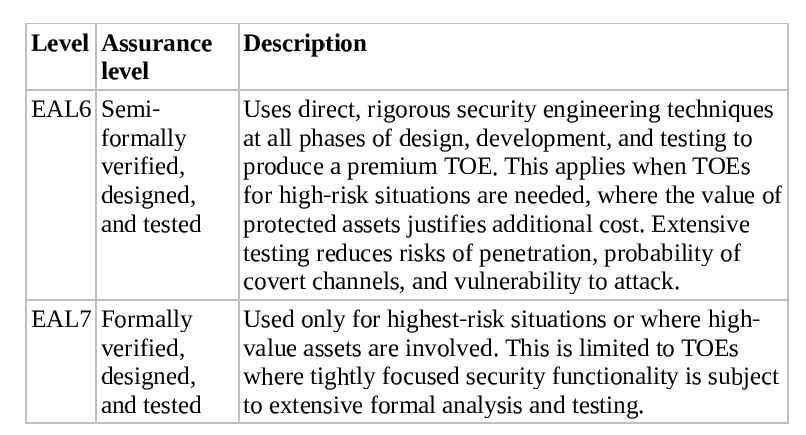
1. Select Controls Based on Systems Security Requirements

Buyers are often willing to consider only systems that have been subjected to formal evaluation processes in advance and have received some kind of security rating.

* 1. Common Criteria (CC): was designed as a dynamic subjective product evaluation model and replaced previous static systems, such as the U.S. Department of Defense’s Trusted Computer System Evaluation Criteria (TCSEC) and the EU’s Information Technology Security Evaluation Criteria (ITSEC). A document titled “**Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security**” was signed by representatives from government organizations in Canada, France, Germany, the UK, and the US in 1998, making the document an international standard. The original arrangement documentation has been formally adopted as a standard and published as ISO/IEC 15408-1, -2, and -3 and primarily labeled as “Information technology -- Security techniques -- Evaluation criteria for IT security.” The objectives of the CC guidelines are as follows:
     1. To add to buyers’ confidence in the security of evaluated IT products
     2. To eliminate duplicate evaluations
     3. To keep making security evaluations more cost-effective and efficient
     4. To make sure evaluations of IT products adhere to high and consistent standards
     5. To promote evaluation and its availability
     6. To evaluate the functionality and assurance of the target of evaluation (**TOE**).

**Protection profiles** (PPs) specify for a TOE the security requirements and protections, which are considered the security desires from a customer. **Security targets** (STs) specify the claims of security from the vendor that are built into a TOE. The client initially selects a vendor based on publised or marketed **evaluation assurance levels** (EALs) for currently available systems. Using CC to choose a vendor allows clients to request exactly what they need for security rather than having to use static fixed security levels.





* 1. Authorize to Operate (ATO): to obtain an official approval to use secured equipment for operational objects. The assessment and assignment of an ATO is performed by an Authorizing Official (AO). Other terms for AO are designated approving authority (DAA), Approving Authority (AA), Security Control Assessor (SCA), and Recommending Official (RO). A typical ATO lasts for 5 years and must be reobtained when:
     1. The ATO time frame has expired
     2. The system experiences a signification security breach or change (decided by the AO)

An AO can issue four types of authorization decisions:

- Authorization to Operate

- Common Control Authorization: when a security control is inherited from another provider and when the risk associated with the common control is acceptable and already has a ATO from the same AO.

- Authorization to Use: when a third-party provider (such as a cloud service) provides IT/IS servers that are deemed to have risk at an acceptable level; it’s also used to allow one AO to accept an ATO granted by another AO.

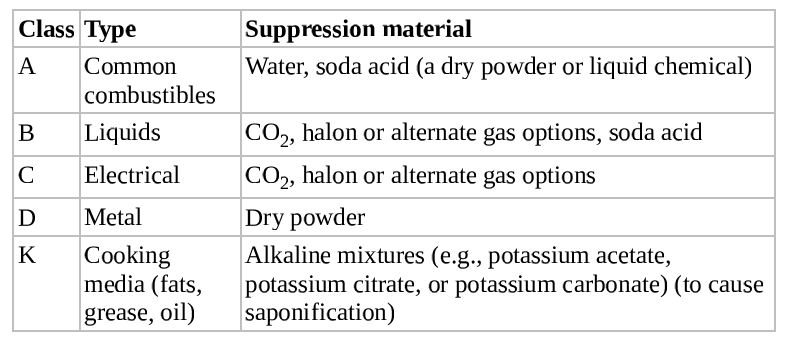
- Denial of Authorization

The RMF ATO concept replace the previous certification and accreditation (C&A) process like C.F.D (Candidates for Deletion).

1. Understand Security Capabilities of Information Systems
   1. Memory Protection: isolation, virtual memory, segmentaion, memory management, and protection rings are discussed in chapter 9. Additionally, memory overflows.
   2. Virtualization: In chapter 9
   3. Trusted Platform Module: already discussed
   4. Interfaces: **constrained** (or **restricited**) **interface** is implemented within an application to restrict what users can do or see based on their privileges. It’s a practical implementation of the Clark-Wilson model of security (which I skipped).
   5. Fault Tolerance: ability of a system to suffer a fault but continue to operate (Chapter 18).
   6. Encryption/Decryption: Chapter 6 and 7
2. Apply Security Principles to Site and Facility Design
   1. Secure Facility Plan: outlines the security needs of your organization and emphasizes methods or mechanisms to employ to provide security. It’s developed through **risk assessment** and **critical path analysis**. Critical path analysis is a systematic effort to identify relationships between mission-critical applications, processes, and operations.
      1. Site Selection
      2. Facility Design:
         1. Guidelines and requirements from Occupational Safety and Health Administration (OSHA) and the Environmental Protection Agency (EPA).
         2. Consider include combustibility, fire rating, construction materials, load rating, placement, and control of items such as walls, doors, ceilings, flooring, HVAC, power, water, sewage, gas, and so on.
         3. Forced intrusion, emergency access, resistance to entry, direction of entries and exits, use of alarms, and conductivity are other important aspects to evaluate.
         4. Crime Prevention Through Environmental Design (CPTED) addresses facility design, landscaping, entrance, concepts, campus layouts, lighting, road placement, and traffic management of vehicles and those on foot.
      3. Implement Site and Facility Security Controls
         1. Administrative physical security controls: facility construction and selection, site management, building design, personnel controls, awareness training, and emergency response and procedures.
         2. Technical physical security controls: building access controls; intrusion detection; alarms; security cameras; monitoring; heating, ventilation, and air-conditioning (HVAC) power supplies; and fire detection and suppression.
         3. Physical controls for physical security include fencing, lighting, locks, construction materials, access control vestibules (mantraps), guard dogs, and security guards.
         4. Wiring Closets:
            1. Entrance facility (demarcation point or MDF): the entrance point to the building where the cable from the provider connects the internal cable plant.
            2. Equipment room: main wiring closet for the building, often connected to or adjacent to the entrace facility
            3. Backbone distribution system: provides wired connections between the equipment room and the telecommunications room, including cross-floor connections
            4. Wiring closet: connection needs of a floor or a section of a large building by providing space for networking equipment and cabling systems.
            5. Horizontal distribution system: provides the connection between the telecommunications room and work areas, often including cabling, cross-connection blocks, patch panels, and supporting hardware infrastructure.

Protected cable distribution or protective distribution systems (PDSs) are the means.

* + - 1. Server Rooms/Data Centers: smart/dumb cards, proximity devices and readers biometrics, IDSs (focusing on physical intruders), and a design based around defense in depth.
      2. Smartcards and Badges: badges maybe color-coded by facility or classification level, and they often include pictures, magnetic stripes, QR codes or bar codes for optical decoding, smartcard chips, RFID, NFC, and personal details to help a security guard verify identity. Smartcards are credit card-sized IDs, badges, or security passes with an embedded magnetic stripe, bar code, or integrated circuit chip. In most cases, they are used in a multifactor configuration.
      3. Proximity device: can be a passive device, a field-powered device, or a transponder to control physical access.
      4. IDS
      5. Noise (mostly electromagnetic noise by wires)
      6. Water: wet pipe system, dry pipe system, preaction system, deluge system
      7. Gas: EPA-approved substitutes for halon. CO2 should be implemented only in special circumstances. Water-based system is inappropriate.
      8. Fire: rate-of-rise detection system, flame-actuated system, smoke-actuated system, incipient smoke detection system



* + - 1. Motion Detectors: digital motion detector monitors, passive infrared (PIR), wave pattern motion detector, capacitance motion detector, photoelectric motion detector, passive audio motion detector
      2. Intrusion alarms: deterrent alarms, repellent alarms, notification alarms, local alarm system, central station system, auxiliary alarm system
      3. Secondary Verification Mechanisms: should be in place after motion detectors, sensors, and alarms are used to prevent false alarms.

1. Establishing Databases and Data Warehousing (chapter 20)
   1. SQL itself is divided into two distinct components: the Data Definition Language (DDL) allowing for the creation and modification of the database’s structure (known as the **schema**) and the Data Manipulation Language (DML) allowing users to interact with the data contained within that schema.
   2. The degree is determined by the number of the columns used in the table. The cardinality is determined by the number of the rows used in the table.
   3. Database Management System Architecture (DBMS): the vast majority of contemporary systems focus relational database management systems (RDBMSs). However, we will also discuss 2 important DBMS architecture: hierarchical and distributed
      1. Hierarchical and Distributed Databases
      2. Relational Databases: The main building block of the relational database is the table (also known as a relation). Each table contains a set of related records. For example, a sales database might contain the following tables:
         1. Customers table that contains contact information for all the organization’s clients
         2. Sales Reps table that contains identity information on the organization’s sales force
         3. Orders table that contains records of orders placed by each customer



Object-Oriented Programming and Databases: OODBs are also better suited than other types of databases for supporting complex applications involving multimedia, CAD, video, graphics, and expert systems.

They are also used to join tables when you wish to cross-reference information. You should be familiar with 3 types of keys:

* + - * 1. Candidate Keys: a subset of attributes that can be used to uniquely identify any record in a table
        2. Primary Keys: selected from the set of candidate keys for a table to be used to uniquely identify the records in a table
        3. Alternate Keys: any candidate key that’s not selected as the primary key
        4. Foreign Keys: enforce relationships between two tables, also known as referential integrity. Ensures that if one table contains a foreign key, it corresponds to a still-existing primary key in the other table in the relationship.

Database Normalization: the process of bringing a database table into compliance with **normal forms** (well-organized and efficient databases) is known as normalization.

Database Transactions: When a transaction successfully finishes, it’s said to be committed to the database and cannot be undone. Transaction committing may be explicit, using SQL’s **COMMIT** command, or it can be implicit if the end of the transaction is successfully reached. If a transaction must be aborted, it can be rolled back explicitly using the **ROLLBACK** command or implicitly if there is a hardware or software failure.

ACID model:

- Atomicity: if any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.

- Consistency: no other transaction should ever be able to use any inconsistent data that might be generated during the execution of another transaction

- Isolation: if a database receives two SQL transactions that modify the same data, one transaction must be completed in its entirety before the other transaction is allowed to modify the same data.

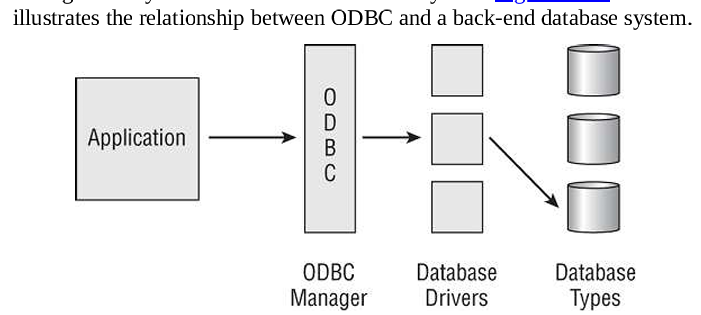
- Durability: databases ensure durability through the use of backup mechanisms, such as transaction logs.

* 1. Security for Multilevel Databases: Often, administrators will deploy a trusted front end to add multilevel security to a legacy or insecure DBMS.

**Database contamination:** mixing data with different classification levels and/or need-to-know requirements.

Restricting Access with Views: **Views** are stored in the database as SQL commands rather than as tables, reducing the space requirements and allowing views to violate the rules of **normalization**. Because of its flexibility, many database administrators use the as a security tool. Users interact only with limited views rather than with the raw tables of data underlying them.

* + 1. Concurrency (or edit control): a preventive security mechanism ensures the information stored in the database is always correct or at least has its integrity and availability protected.
       1. Lost Updates: occur when 2 different processes make updates to a database, unaware of each other’s activity
       2. Dirty Reads: occur when a process reads a record from a transaction that did not successfully commit.
    2. Aggregation: SQL provides a number of functions that combine records from one or more tables to produce potentially useful information. It’s especially important for database security administrators to strictly control access to aggregate functions and adequately assess the potential information they may reveal to unauthorized individuals.
    3. Inference: combine several pieces of nonsensitive information to gain access to information that should be classified at a higher level. However, it makes use of the human mind’s deductive capacity rather than the raw mathematical ability of modem database platforms. **Database partitioning** may help subvert these attacks.
    4. Other Security Mechanisms
       1. Administrators may employ time and date stamps to maintain data integrity and availability
       2. Objects can be controlled granularly within the database.
          1. Content-dependent access control: based on the contents or payload of the object being accessed.
          2. Cell suppression: hiding individual database fields or cells or imposing more security restrictions on them.
       3. Context-dependent access control: evaluates the big picture to make access control decisions. Any single element may look innocuous by itself, but in a larger context that element may be revealed to be benign or malign.
       4. Database partitioning: splitting a single database into multiple parts, each with a unique and distinct security level or type of content.
       5. Polyinstantiation: occurs when two or more rows in the same relational database table appear to have identical primary key elements but contain different data for use at differing classification levels.
       6. Inserting false and misleading data into a DBMS (also known as **noise and perturbation**).
  1. Open Database Connectivity: a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type.



* 1. NoSQL
     1. Key/value stores: the simpliest possible form of database, useful for high-speed applications
     2. Graph databases: store data in graph format using nodes to represent objects and edges to represent relationships
     3. Document stores: store **complex** (is in the form of a document like XML and JSON) information using keys.

Domain 4: Communication and Network Security

1. Chapter 11: Secure Network Architecture and Components
   1. OSI model.
      1. Peer layer communication: the information removed by each layer contains instructions, checksums, and so on that can be understood only by the peer layer that originally added or created the information.
      2. Protocol data unit (PDU): a network container that encapsulates data at layer 5, 6, and 7.
      3. TCP/UDP: layer 4.
      4. Packet: layer 3
      5. Frame: layer 2
      6. Bits: layer 1
      7. Application layer: the protocols and services required to transmit files, exchange messages, connect to remote terminals, and so on.
      8. Presentation layer: responsible for transforming data into a format that any system following the OSI model can understand.

Encryption in relation to network communication can occur in at least five locations:

* + - 1. Pre-network encryption where the software encrypts prior to sending the data into the Application layer
      2. TLS for Transport
      3. VPN at layer 2, 3, or 4 such as L2TP, IPsec, or OpenVPN, respectively.
      4. Wireless encryption at the Data Link layer
      5. Bulk encryption at Physical layer (device external to the NIC).
    1. Session layer: establishing, maintaining, and terminating communication sessions between two computers. Manages **dialog discipline** or **dialog control** (simplex, half-duplex, full-duplex). Establishes checkpoints for grouping and recovery, and retransmits PDUs that have failed.
       1. Simplex: one-way communication
       2. Half-duplex: two-way communication, but only one direction can send data at a time.
  1. TCP/IP: Application, Transport, Internet, and Link layers.
  2. Protocol analyzer: same as sniffer, network evaluator, network analyzer, traffic monitor, or packet-capturing utility.
     1. Port:
        1. Telnet/tcp: 23 (not recommed, use ssh instead)
        2. FTP/tcp: 20 for active mode, 21 for passive mode
        3. TFTP/udp: 69
        4. SMTP/tcp: (not recommend, recommend SMTPS cuz it has TLS) used for transmit email, 25.
        5. POP3 (Post Office Protocol)/tcp: used to pull email messages from an inbox, 110 (recommend POPS)
        6. IMAP4 (Internet Message Access Protocol)/tcp: (recommend IMAPS) same usage as POP and can retrieve only headers or delete messages directly off the email server (**server arching**), 143.
        7. DHCP, udp: 67
        8. HTTP, tcp: 80
        9. HTTPS, tcp: 443
        10. LPD (Line printer Daemon), tcp: 515, recommend enclosed data in VPN
        11. X Window, tcp: 6000-6063 (recommend use with VPN).
        12. NFS (Network File System), tcp: network service that supports file sharing between dissimilar systems, 2049 (recommend use with VPN).
        13. SNMP, udp: used to collect network health and status information, 161 (162 for **Trap Messages**) (recommend SNMPv3 only). 161 is used by the SNMP agent (network device) to receive requests while 162 is used by the mangement console to receive responses and notifications (trap messages).
     2. Transport layer: port number ranges from 0 to 65535 (2^16).
        1. Socket: a combination of an IP address and a port number
        2. Multiplexing over IP: ports allow a single IP address to be able to support multiple simultaneous communications.
        3. Well-known ports or service ports (exclusively used by servers): 0-1,023
        4. Registered software ports (registered with the International Assigned Numbers Authority IANA): 1,024 to 49,151
        5. Random, dynamic, or ephemeral ports (used randomly by clients as a source port): 49,152 to 65,535. However, most OSs allow for any port from 1,024 to be used as a dynamic client source port as long as it is not already in use on that local system.
        6. DNS: links IP addresses and human-friendly fully qualified domain names (FQDNs) together. An FQDN consists of three main parts:
           1. Top-level domain (TLD)-the com in [www.google.com](http://www.google.com)
           2. Registered domain name-the google in [www.google.com](http://www.google.com)
           3. Subdomain(s) or hostname-the www in [www.google.com](http://www.google.com)
        7. Zone file: collection of resource records or details about the specific domain. Dozens of these can be found on [www.iana.org/assignments/dns-parameters/dns-parameters.xhtml](http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml) such as A records linking an FQDN to an IPv4 address and AAAA records linking an FQDN to an IPv6 address.
        8. Every registered domain name has an assigned authoritative name server.
           1. Primary authoritative name server: hosts the original editable zone file for the domain
           2. Secondary authoritative name server: can be used to host read-only copies of the zone file.
        9. DNSSEC (dnssec.net): a security improvement to the existing DNS infrastructure. Provide mutual certificate authentication and encrypted sessions between devices during DNS operations. It has been widely adopted and can prevent **zone file poisoning** and **DNS cache poisoning**.
        10. Non-DNS servers (mostly client devices) should consider using **DNS over HTTPS** (DoH), creating encrypted session with a DNS server of TLS-protected HTTP which is used (the encrypted session) as a VPN to protect the DNS query and response. **Oblivious DoH** (ODoH) is the late 2020 enhancement of DoH, adding a DNS proxy between the client and the DNS resolver so that the identity of the requesting client is isolated from the DNS resolver.
        11. Rogue DNS Server: capture any DNS query or specific one then send the false IP information.
        12. Performing DNS Cache Poisoning: attackers focus on caching real DNS servers or clients (storing false DNS records into their system).
        13. DNS Pharming: malicious redirection of a valid website’s URL or IP address to a **fake website**. Occurs by modifying the locat hosts file or DNS poisoning/spoofing DNS resolution.
        14. Altering the Hosts file (stored on individual end-point).
        15. Corrupt the IP configuration: the DNS server address is typically distributed to clients through DHCP, but it can also be assigned statically. Attacks to alter a client’s DNS server lookup address can be performed by compromising DHCP or through a script.
        16. DNS Query Spoofing: eavesdrop DNS query then spoof.
        17. Proxy falsification: although not strictly a DNS issue, a proxy falsification attack could be implemented via DNS if the proxy’s domain name has to be resolved by the client to use the proxy. *Many organizations use a proxy server to filter traffic, enforce policies, or improve security. The proxy server is typically accessed using a domain name (e.g., proxy.company.com).*
        18. Zone transfer: the process of copying DNS zone files from one DNS server to another. This is mainly used to synchronize DNS records between a primary (master) DNS server and a secondary (slave) DNS server to ensure redundancy and availability.
        19. Defense to DNS poisoning:
            1. Limit zone transfer from internal DNS servers to external DNS servers (blocking inbound TCP port 53 (zone transfer requests) and inbound UDP port 53 (queries)).
            2. Require internal clients to resolve all domain names through the internal DNS (blocking outbound UPD port 53 while keeping open outbound TCP port 53).
            3. Limit the external DNS servers from which internal DNS servers pull zone transfers.
            4. Deploy a network IDS (NIDS) & install HIDS.
            5. Use DNSSEC, DoH, or ODoH on all clients where supported.
            6. DNS sinkhole: a specific example of a false telemetry system (aka sinkhole server, internet sinkhole, and blackhole DNS), an effectively DNS spoofing used as a defense. It provides false responses to DNS queries from malware, such as bots, to prevent access to command and control systems.
        20. Domain Hijacking (or domain theft): XSRF, hijecking a session, using an on-path/MitM attack, or exploiting a flaw in the domain registrar’s systems.
            1. Best defense: use strong multifactor authentication when logging into your domain registrar.
            2. Defense against letting your domain registration lapse (fails to renew domain name before the expiration date): set up auto-renew and double-check the payment method a week before the renewal date.
        21. Typosquatting: when users mistypes the domain name or IP address
        22. Homograph attack: for example, in many fonts, some letters in Cyrillic look like Latin characters; for example, the l (I.e., lowercase L) in Latin looks like the Palochka Cyrillic letter.
        23. URL hijacking
        24. Clickjacking: any mouse click or selection will be captured by the floating frame and redirected
     3. Internet Protocol (IP) Networking: it was designed to perform “best effort” in finding a path or route to a destination, in spite of a damaged or corrupted network structure. Thus, you must employ TCP with IP to gain reliable and controlled communication sessions.
        1. IPv4 (32-bit) vs IPv6 (128-bit):
           1. Autoconfiguration removes the need for both DHCP and NAT. It works on IPv6 and the security is handled by firewall rules instead of NAT compared to IPv4. Also, IPsec is native to IPv6, but it is an add-on for IPv4. Some of IPv6’s new features are scoped addresses, autoconfiguration, and quality of service (QoS) priority values. Scoped addresses give administrators the ability to group and then bock or allow access to network services, such as file servers or printing. QoS priority values allow for traffic management based on prioritized content (IPv4 has ToS-Type of Services but it seemed to go unused and was converted into the Differentiated Services-DS by later specification).
           2. Migration to IPv6 raises several security concerns:

IP filtering and block lists will be less effective because of more IP addresses.

Secure deployment of IPv6 requires security filtering and monitoring products be upgraded. Otherwise, it will serve as a covert channel.

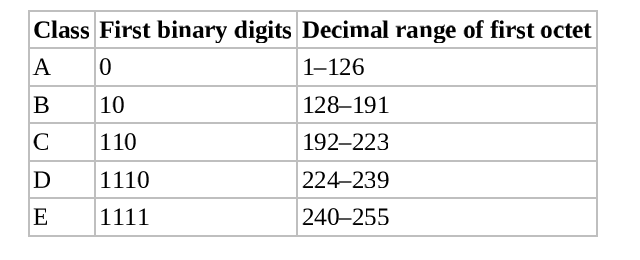
Loss or lack of NAT. NAT is not necessary and isn’t addressed in the specification. Privacy is lost or reduced without NAT since a system’s locally assigned IP address is not masked by NAT to a public address. Most networks already using stateful inspection firewall in addition to NAT in IPv4 network.

* + - * 1. For IPv6 and IPv4 coexist:

Dual stack: having systems operate both IPv4 and IPv6 and using the appropriate protocol for each conversation.

Tunneling: allows most systems to operate a single stack of either IPv4 or IPv6 and use an encapsulation tunnel to access systems of the other protocol.

NAT-PT (RFC-2766) (Network Address Translation-Protocol Translation): used to convert between IPv4 and IPv6 network segments similar to how NAT converts internal and external addresses.

* + - * 1. IPv4 classes:
        2. CIDR notation: using /16 instead of 255.255.0.0 as a subnet mask representation for example.
        3. ICMP: unfortunately, its features were often exploited in various forms of bandwidth-based DoS attacks, such as **ping of death**, **smurf attacks,** and **ping floods**. This fact has shaped how networks handle ICMP traffic today.
        4. IGMP: allows systems to support multicasting. **RFC 1112** discusses the requirements to perform IGMP multicasting.
        5. ARP:

Best defense: port security on the switch, local or software firewall, HIDPS, or sepcial endpoint security products to block unrequested ARP replies/announcements. One popular tool used to detect ARP poisoning is **arpwatch**.

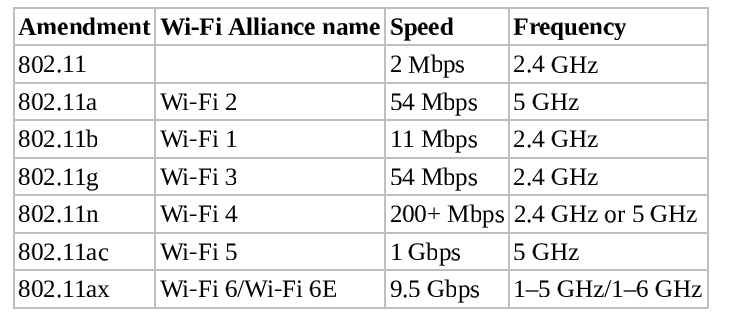
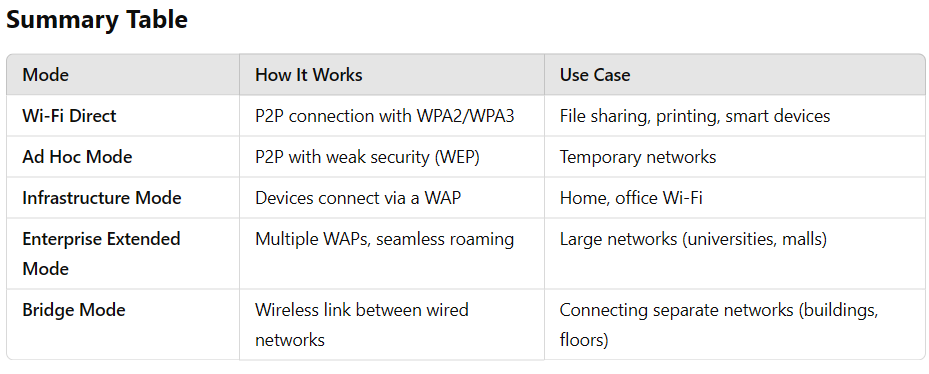
Another defense: static ARP entries.

* + 1. Secure Communication Protocols
       1. IPsec: a standard of IP security extensions used as an add-on for IPv4 and integrated into IPv6.
       2. Kerberos: offers a SSO solution for users and provides protection for logon credentials. Kerberos is discussed further in chapter 14.
       3. SSH: can be used to encrypt numerous plaintext utilities (like **rcp, rlogin,** and **rexe**), serve as a protocol encrypter (such as with SFTP), and function as a transport mode VPN.
       4. Signal Protocol: a cryptographic protocol that provides end-to-end encryption for voice communications, videoconferencing, and text message services. It’s **nonfederated**.
       5. Secure Remote Procedure Call (S-RPC): an authentication service for cross-network service communications, preventing unauthorized execution of code on remote systems.
       6. Transport Layer Security (TLS): TLS operates at OSI layer 4 but it can encrypt any Application layer protocol. TLS replaced SSL.
          1. Often implemented as the initial payload of a TCP packages, allowing it to encapsulate all higher-layer protocol payloads.
          2. Can be used to encrypt UDP and SIP (session initiation protocol, a protocol that is associated with VoIP) connections.
       7. VPN: [ Ethernet [ IPsec [ IP [ TCP [ TLS [ HTTP [Payload] ] ] ] ] ] ]
       8. Encapsulation is not always implemented for benign purposes. Numerous covert channel communication mechanisms use encapsulation to hide or isolate an unauthorized protocol inside another authorized one.
          1. For example, if a network blocks the use of FTP but allows HTTP, then tools such as **HTTPTunnel** can be used to bypass this restriction: [ Ethernet [ IP [ TCP [ HTTP [ FTP [Payload] ] ] ] ].
          2. Another example, with utilities such as **Loki**, ICMP is transformed into a tunnel protocol to support TCP communications: [Ethernet [ IP [ ICMP [ TCP [ HTTP [Payload] ] ] ] ] ]
          3. **Unbouded encapsulation support**: ability to jump between VLANs.
       9. Few drawbacks of multilayer protocols:
          1. Covert channels are allowed
          2. Filters can be bypassed
          3. Logically imposed network segment boundaries can be overstepped.
       10. DNP3 (Distributed Network Protocol 3): primarily used in the electric and water utility and management industries. It’s used to support communications between data acquisition systems and the system control equipment: substation computers, remote terminal units (RTUs) (I.e., devices controlled by an embedded microprocessor), intelligent electronic devices (IEDs), and SCADA primary stations (i.e., control centers) [www.dnp.org/About/Overview-of-DNP3-Protocol](http://www.dnp.org/About/Overview-of-DNP3-Protocol)
    2. Converged Protocols: merging of specialty or proprietary protocols with standard protocols like those from TCP/IP suite. Primary benefit: able to use existing TCP/IP supporting network infrastructure to host special or proprietary services without the need for unique deployments of alternate networking hardware.
       1. Storage Area Network (SAN): secondary network, consolidating network-accessible storage container. It’s often used to enhance networked storage devices such as hard drives, drive arrays, optical jukeboxes, and tape libraries so that they can be made to appear to servers as if they were local storage. Sans operate by encapsulating or converging data storage signals into TCP/IP communications in order to separate storage and proximity. A SAN can be a single point of failure, so redundancy needs to be integrated to provide protection of availability. In some instances, a SAN may implement deduplication in order to save space by not retaining multi copies of the same file. However, this can sometimes result in data loss if the one retained original is corrupted.
       2. Fibre Channel over Ethernet (FCoE): Fibre Channel: a form of network data-storage solution (SAN or network-attached storage [NAS]) that allows for high-speed file transfer upward of 128 Gbps. It operates at layer 2. It’s was designed to be operated over fiber-optic cables; support for copper cables was added later to offer less expensive options. It typically requires its own dedicated infrastructure (separate cables). However, FCoE can be used to support it over the existing network infrastructure. FCoE is used to encapsulate Fibre Channel communications over Ethernet networks. It typically requires 10 Gbps Ethernet in order to support the Fibre Channel protocol. With this technology, Fibre Channel operates as a Network layer or OSI layer 3 protocol, replacing IP as the payload of a standard Ethernet network. Fibre Channel over IP (FCIP) further expands the use of Fibre Channel signaling to no longer require any specific speed of network. It’s the SAN equivalent of VoIP.
       3. MPLS (Multiprotocol Label Switching): a high-throughput high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. This technique saves significant time over tranditional IP-based routing processes, which can be quite complex. Furthermore, MPLS is designed to handle a wide range of protocols through encapsulation. Thus, the network is not limited to TCP/IP and compatible protocols. This enables the use of many other networking technologies, including T1/E1, ATM, Frame Relay, SONET, and Digital Subscriber Line (DSL).
       4. Internet Small Compuer System Interface (iSCSI) Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP that operates at layer 3. This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public internet connections. iSCSI is often viewed as a low-cost alternative to Fibre Channel.
    3. VoIP: a tunneling mechanism that encapsulates audio, video, and other data into IP packets to support voice calls and multimedia collaboration. It’s inexpensive telephony solution for companies and individuals worldwide. Some VoIP solutions are software only (Skype) and somes require specialized hardware to either replace tranditional telephone handsets/base stations or allow these to connect to and functions over the VoIP system. Hackers can wage a wide range of potential attacks against a VoIP solution:
       1. Caller ID can be falsified easily using any number of VoIP tools, so hackers can perform vishing (VoIP phishing) or Spam over Internet Telephony (SPIT) attacks.
       2. The call manager systems and VoIP phones themselves might be a vulnerable to host operating system attacks and DoS attacks. If a device’s or software’s host OS or firmware has vulnerabilities, there is increased risk of exploits.
       3. Attackers might be able to perform MitM/on-path attacks by spoofing call managers or endpoint connection negotiations and/or responses.
       4. Depending on the deployment, there are also risks associated with deploying VoIP phones off the same switches as desktop and server systems. This could allow for 802.1X authentication falsification as well as VLAN and VoIP hopping (i.e., jumping across authenticated channels).
       5. Since VoIP traffic is just network traffic, it’s often possible to listen in on VoIP communications by decoding the VoIP traffic when it isn’t encrypted.

Secure Real-Time Transport Protocol or Secure RTP (SRTP) is a security improvement over the Real-Time Transport Protocol (RTP) that is used in many VoIP communications. SRTP aims to minimize the risk of DoS, on-path attacks, and other VoIP exploits through robust encryption and reliable authentication. RTP or SRTP takes over after Session Initiation Protocol (SIP) establishes the communication link between endpoints.

* + 1. Software-Defined Networking (SDN):
       1. The concept is based on the theory that the complexities of a traditional network with on-device configuration (i.e., routers and switches) often force an organization to stick with a single device vendor, and limit the flexibility of the network to adapt to changing physical and business conditions, as well as optimize costs of acquiring new devices.
       2. It aims at separating the **infrastructure layer** (aka the data plane and the forwarding plane)--hardware and hardware-based settings--from the control layer--network services of data transmission management.
       3. The control plane uses protocols to decide where to send traffic, and the data plane includes rules that decide whether traffic will be forwarded.
       4. This form of traffic management also involves access control over what systems can communicate which protocols to whom. This type of access control is typically attribute-based access control (ABAC) focused or based.
       5. SDN gives the option to handle traffic routing using simpler network devices that accept instructions from the SDN controller. This eliminates some of the complexity related to traditional networking protocols and concepts: IP addressing, subnets, routing, and the like from needing to be programmed into or be deciphered by hosted applications.
       6. Using SDN frees an organization from having to purchase devices from a single vendor. The configuration and management of hardware are then controlled through a centralized management interface. In addition, the settings applied to the hardware can be changed and adjusted dynamically as needed.
       7. It allows data transmission paths, communication decision trees, and flow control to be virtualized in the SDN control layer rather than being handled on the hardware on a per-device basis.
       8. SAN is a network technology that combines multiple individual storage devices into a single consolidated network-accessible storage container. They are often used with multiple or clustered servers that need high-speed access to a single shared dataset. These have historically been expensive due to the complex hardware requirements of the SAN.
       9. Virtual SAN (VSAN) bypass the complexities of the SAN with virtualization. A virtual SAN or a software-defined shared storage system is a virtual re-creation of a SAN on top of a virtualized network or an SDN.
       10. Software-defined storage (SDS) is another derivative of SDN. SDS is a SDN version of a SAN or NAS. SDS is a storage management and provisioning solution that is policy driven and is independent of the actual underlying storage hardware. It’s effectively virtual storage.
       11. Software-defined wide-area networks (SDWAN or SD-WAN) is an evolution of SDN that can be used to manage the connectivity and control services between distant data centers, remote locations, and cloud services over WAN links.
    2. Microsegmentation: is dividing an internal network into numerous subzones, potentially as small as a single deice, such as a high-value server or event a client or endpoint device. Each zone is separated from the others by internal segmentation firewalls (ISFWs), subnets, VLANs, or other virtual networking solutions. Microsegmetation is a key element in implementing zero trust.
       1. Boosting Performance Network
       2. Reducing Communication Problems
       3. Providing Security

Another often-overlooked network segmentation concept is the creation of an out-of-band pathway. This is often performed to create a separate and distinct network structure for traffic that would otherwise interfere with the production network or that may itself be put at risk if placed on the production network. Secondary (or additional) network paths or segments may be created to support data storage traffic (such as with SANs), VoIP, backup data, patch distribution, and mangement operations.

* + 1. Virtual eXtensible LAN (VXLAN) enables VLANs to be stretched across subnets and geographic distances.
    2. Wireless network: can be deployed in either ad hoc mode or infrastructure mode. 
       1. **Wi-Fi Direct** is an upgraded version of ad hoc mode that can support WPA2 and WPA3 (ad hoc supported only WEP).
       2. Infrastructure mode means that a wireless access point (WAP) is required and restrictions for wireless network access are enforced.
       3. An **enterprise extended mode** deployment is when multiple wireless access point (WAPs) are used to connect a large physical area to the same wired network. Each WAP will use the same **extended service set identifier** (**ESSID**) so that clients can roam the area while maintaining network connectivity, even while their wireless NICs change associations from one WAP to another.
       4. A **bridge mode** deployment is when a wireless connection is used to link two wired networks. This often uses dedicated wireless bridges and is used when wired bridges are inconvenient, such as when linking networks between floors or building.
       5. A **fat access point** is a base station that is a fully managed wireless system, which operates as a standalone wireless solution. A **thin access point** is little more than a wireless transmitter/receiver, which must be managed from a separate external centralized management console called a **wireless controller**.
    3. Securing the SSID
       1. Wireless networks are assigned a SSID to differentiate one wireless network from another. There are 2 types of infrastructure mode SSIDs:
          1. ESSID (extended SSID): name of a wireless network when a WAP is used.
          2. BSSID (basic SSID): MAC address of the base station, which is used to differentiate multiple base stations supporting an ESSID.

ISSID (Independent SSID): used by Wi-Fi Direct or ad hoc mode.

* + - * 1. If a wireless client knows the SSID, they can configure their wireless NIC to communicate with the associated WAP. Knowledge of the SSID does not always grant entry, though, because the WAP can use numerous security features to block unwanted access.
        2. SSID are defined by default by vendors and thus are well known. Standard security practice dictates that the SSID should be changed to something unique before deployment
        3. Beacon frame: the SSID broadcast by the WAP. This default broadcast can be disabled to attempt to keep the wireless network secret. However, attackers can still use wireless sniffer since the SSID is still used in transmissions between connected wireless clients and the WAP. Instead, use WPA2 or WPA3 rather than trying to hide the network.
      1. Wireless channels: Think of channels as lanes on the same highway. To avoid channel overlap interference, configure nearby access points to use non-overlapping channels whenever possible. This means that if APs are close to each other, they should be set to different channels that do not interfere. For example, in the 2.4 GHz Wi-Fi band, the non-overlapping channels are 1, 6, and 11. 5 GHz wireless was designed to avoid this channel overlap and interference issue. While 2.4 GHz channels are 22 MHz wide and 5 MHz apart, 5 GHz channels are 20 MHz wide and 20 MHz apart. Therefore, adjacent 5 GHz channels do not interfere with one another. Furthermore, adjacent channels can be combined or bonded into a larger width channel for faster throughput.
         1. US: 11 channels defined within the 2.4 GHz frequency range
         2. Europe: 13 channels
         3. Japan: 14 channels

5GHz is often preferred for internal networks. Most of the mesh Wi-Fi options are based on 5 GHz and use three or more mini-WAP devices to provide ML-optimized coverage throughout a home or office. There is 6 GHz that provides for more top-speed connections than earlier forms of Wi-Fi. However, 6 GHz is even more restricted by obstacles and distance.

* + - 1. Conducting a Site Survey
         1. Site survey: a formal assessment of wireless signal strength, quality, and interference using an RF signal detector
         2. Heat map: a mapping of signal strength measurements over a building’s blueprint
         3. Hot spots: oversaturation of signal
         4. Cold spots: lack of signal
      2. Wireless security:
         1. Encryption is only between the client device and the base station.
         2. Use a VPN for end-to-end encryption.
         3. The original IEEE 802.11 defined two methods that wireless clients can use to authenticate to WAPs before normal network communications can occur across the wireless link.

OSA (open system authentication): no real authentication is required

SKA (shared key authentication). The 802.11 standard defines one optional technique for SKA known as Wired Equivalent Privacy (WEP). Later amendments add WPA, WPA2, WPA3, and others.

* + - * 1. Common AAA services: UDP 1812 for RADIUS and TCP 49 for TACACS+
        2. Extensible Authentication Protocol (EAP): an authentication framework
        3. LEAP (Lightweight Extensible Authentication Protocol): Cisco proprietary alternative to TKIP for WPA
        4. PEAP (Protected Extensible Authentication Protocol): encapsulates EAP methods within a TLS tunnel.
        5. WPS (Wi-Fi Protected Setup): a security standard for wireless networks. Operates by auto-connecting and automatically authenticating the first new wireless client to initiate a connection to the network once WPS is triggered (by a button on the WAP or a code or PIN that can be sent to the base station remotely).
        6. Wireless MAC Filter: can be used on a WAP to limit or restrict access
        7. Wireless Antenna Management: can be used for wireless clients and base stations

Pole or straight antenna: omnidirectional antenna

Directional antennas: Yagi, cantenna, panel, and parabolic

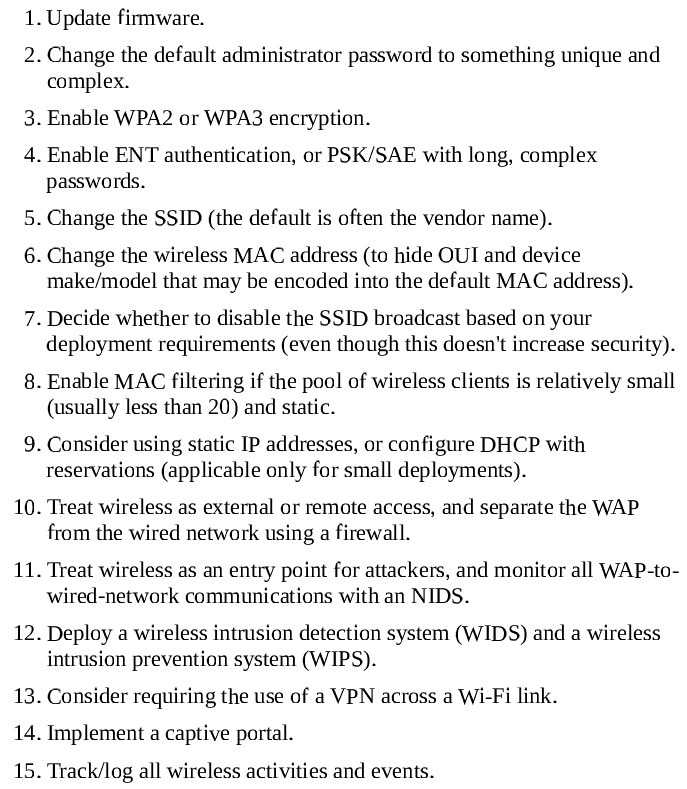
Consider this guidelines:

Use a central location

Avoid solid physical obstructions

Avoid reflective or other flat metal surfaces

Avoid electrical equipment.

* + - * 1. Captive Portals: an authentication technique that redirects a newly connected client to a web-based portal access control page. Most located at hotels, restaurants, bars, airports, libraries, and so on. The **portal page** may require the user to input payment information, provide logon credentials, or input an access code. Also used to display AUP, privacy policy, and tracking policy to the user, who must consent to the policies before being able to communicate across the network.
        2. General Wi-Fi Security Procedure:
        3. Wireless Communications:

To manage the simultaneous use of the limited radio frequencies, several alternative spectrum-use techniques were developed:

Spread spectrum: a message is broken into pieces sent at the same time at different frequency

FHSS: like spread spectrum but only one frequency at a time

DSSS: use **chipping code** to allow a receiver to reconstruct data

OFDM: requires a smaller frequency set (channel bands) to employs a digital multicarrier modulation (perpendicular/orthogonal modulated signals) scheme that allows for a more tightly compacted transmission.

Bluetooth: defined in IEEE 802.15 and uses the 2.4 GHz. It suffers to a wide range of attacks

Bluesniffing

Bluesmacking

Bluejacking

Bluesnarfing: it’s possible against nondiscoverable devices if their Bluetooth MAC addresses are known, which could be gathered using bluesniffing.

Bluebugging

Best defense: just minimize the use in public

RFID:

NFC (near-field communication): a standard that establishes radio communications between devices in close proximity

* + - * 1. Wireless attacks:

Wi-Fi scanners: detect wireless network even SSID broadcast disabled.

Rogue access points: should be discovered and removed

Evil Twin

Disassociation: disconnect a client from one WAP

Network with hidden SSIDs: disassociation packet with a MAC address spoofed as that of the WAP is sent to a connected client that causes the client to lose its connection and then send a Reassociation Request packet, which includes the SSID in the clear.

An attack can send repeated disassociation frame to a client to prevent reassociation thus causing a DoS.

A session hijack event can be initiated by using diassociation frames to keep the client disconnected while the attacker impersonates the client and takes over their wireless session with the WAP.

An on-path attack can be implemented by using a disassociation frame to disconnect a client. Then the attacker provides a stronger singal from their rogue/fake WAP using the same SSID and MAC as the original WAP; once the client connects to the false WAP, the attacker connects to the valid WAP.

Best defense is to operate a WIDS, which monitors for wireless abuses.

Jamming: to avoid or minimize interference and jamming, start by adjusting the physical location of devices. Next, check for devices using the same frequency and/or channel. If there are conflicts, change the frequency or channel in use on devices you control.

IV (initialization vector) abuse: for example, cracking WEP encryption using the wesside-ng tool from the Aircrack-ng suite at aircrack-ng.org.

Replay

Other Communication Protocols

LiFi (light fidelity)

Satellite communications

Narrow-band wireless is widely used by SCADA

Zigbee: an IoT equipment communications concept that is based on Bluetooth

Cellular Networks: 2G, 3G, 4G, 5G (latest)

Content Distribution Networks (CDNs)

Secure Operation of Hardware

Common Network Equipment

Repeaters, concentrators, amplifiers…

Sensor: collects information and then transits it back to a central system for storage and analysis, common for fog computing, ICS, IoT, IDS/IPS, and SIEM/security orchestration, automation, and response (SOAR) solutions.

Collector: any system that gathers data into a log or record file.

Aggregators: type of multiplexor.

Network Access Control (NAC): concept of controlling access to an environment through strict adherence to and enforcement of security policy. Originally, 802.1X (which provides port-based NAC) was thought to embody NAC, but most supporters believe that 802.1X is only a simple form of NAC or just one optional component in a complete NAC solution. NAC can be implemented with a preadmission philosophy or a postadmission philosophy, or aspects of both:

The preadmission philosophy requires a system to meet all current security requirements (such as patch application and malware scanner updates) before it is allowed to communicate with the network

The postadmission phlosophy allows and denies access based on user activity, which is based on a predefined authorization matrix.

Carrier-Sense multiple access (CSMA): the LAN media access technology that performs communications using these steps:

The host listens to the LAN media to determine whether it is in use

If the LAN media is not being used, the host transmits its communication

The host waits for an acknowledgment

If no acknowledgment is received after a time-out period, the host starts over at step 1.

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD): also LAN media access technology

The host listens to the LAN media to determine whether it is in use

If the LAN media is not being used, the host transmits its communication

While transmitting, the host listens for collisions (in other words, two or more hosts transmitting simultaneously).

If a collision is detected, the host transmits a jam signal.

If a jam signal is received, all hosts stop transmitting. Each host waits a random period of time and then starts over at step 1.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA): also LAN media access technology

The host has two connections to the LAN media: inbound and outbound. The host listens on the inbound connection to determine whether the LAN media is in use.

If the LAN media is not being used, the host requests permission to transmit.

If permission is not granted after a time-out period, the host starts over at step 1.

If permission is granted, the host transmits its communication over the outbound connection.

The host waits for an acknowledgement.

If no acknowledgement is received after a time-out period, the host starts over at step 1.

Token Passing: LAN media access technology that performs communications using a digital token. Token passing was used by ring topology-based networks, such as legacy Token Ring and Fiber Distributed Data Interface (FDDI). Token passing prevents collisions since only the system possessing the token is allowed to transmit data.

Polling: LAN media access technology that … using a primary-secondary configuration. Polling can be configured to grant one system (or more) priority over other systems. For example, if the standard polling pattern was 1,2,3,4, then to give system 1 priority, the polling pattern could be changed to 1,2,1,3,1,4

Chapter 12:

1. Assess and implement secure design principles in network architectures
   1. Internet Protocol (IP) networking (e.g., Internet Protocol Security IPsec)
   2. Internet Protocol (IP) v4/6
2. Implement secure communication channels according to design
   1. Voice
   2. Multimedia collaboration
   3. Remote access
   4. Data communications
   5. Virtualized networks
   6. Third-party connectivity

Blockchain and cryptocurrency regulations are rapidly evolving areas of law and compliance. Here’s an overview to help you get started:

### ****1. Key Regulatory Bodies and Frameworks****

**U.S. SEC (Securities and Exchange Commission)**  
The SEC has played a significant role in regulating cryptocurrencies, especially in terms of whether certain tokens qualify as **securities** under the Howey Test. If a cryptocurrency is considered a security, it must comply with securities laws, including registration requirements. For example, **Initial Coin Offerings (ICOs)** can face scrutiny if they are found to involve unregistered securities.

**CFTC (Commodity Futures Trading Commission)**  
The **CFTC** has jurisdiction over certain cryptocurrencies when they are considered **commodities**, like Bitcoin. It has the authority to regulate the trading of cryptocurrency futures, such as those listed on exchanges like the CME (Chicago Mercantile Exchange).

**FATF (Financial Action Task Force)**  
The **FATF** provides international guidelines for **anti-money laundering (AML)** and **counter-financing of terrorism (CFT)** regulations. Its **Travel Rule** requires crypto businesses to share sender and recipient information for transactions above a certain threshold, similar to how traditional financial institutions operate.

Chapter 13:

1. Controlling Access to Assets
   1. In additional to personnel, assets can be these:
      1. Information: Logical access controls attempt to prevent unauthorized access to the information.
      2. Systems: IT systems that provide one or more services like a simple file server that stores user files is a system. Additionally, a web server working with a database server to provide an ecommerce service is a system. Permissions assigned to user and system accounts **control system access**.
      3. Devices: computing system (like routers, switches, smartphones, and external devices such as printers). Organizations have increasingly adopted policies allowing employees to connect their personally owned devices (such as smartphones or tablets) to an organization’s network. Although the employees may own the devices, organizational data stored on the devices is still an asset of the organization.
      4. Facilities: physical location that it owns or rents (individual rooms, entire buildings, or whole complexes of several buildings). **Physical security controls** help protect facilities.
      5. Applications: provide access to an organization’s data. Permissions are an easy way to restrict logical access to applications and be assigned to specific users or groups.
2. Controlling Physical and Logical Access
   1. Physical Security Requirements (Chapter 10):
      1. Perimeter security controls: fences, gates, guards, turnstiles
      2. Environmental controls: HVAC and fire suppression.
      3. Organizations often have a server room where servers are running (commonly have routers and switches).
      4. Desktop computers typically aren’t as valuable as servers, but regular physical security controls such as locks provide protection.
   2. Logical access controls: used to protect access to information, systems, devices, and applications. They includes these:
      1. Authentication
      2. Authorization
      3. Permissions

Similarly, they restrict access to configuration settings on systems and network devices to only authorized individuals. Many of these logical access controls can apply to resources on site or in the cloud.

1. The CIA Triad and Access Controls.
2. Managing Identification and Authentication
   1. Identification: A core principle with authentication is that all subjects must have unique identities.
   2. Authentication: the authentication information used to verify identity is private and needs to be protected. As an example, passwords are rarely stored in clear text within a database.
   3. The roles of subject and object can switch back and forth (like programs, services, and computers for example).
   4. Registration, Proofing, and Establishment of Identity
      1. Acceptable documentation for in-person identity proofing includes: passport, driver’s license, birth certificate, and more.
      2. After verifying the documents, employees (from the HR department) begin the registration process.
      3. Online organizations often use knowledge-based authentication (KBA) for identity proofing of someone new.
      4. Cognitive password (security questions): used when a known user is trying to change a password. One flaw is that the information is often available on social media sites or with internet searches. **NIST SP 800-63B** “Digital Identity Guidelines: Authentication and Lifecycle Management” discourages using these static questions.
      5. Authorization and Accountability: Identification and authentication are “all-or-nothing” aspects of access control. Either a user’s credentials prove a professed identity, or they don’t. In contrast:
         1. Authorization: occupies a wide range of variations. For example, a user may be able to read a file but not delete it, or they may be able to print a document but not alter the print queue.
         2. Accountability: like auditing, logging, and monitoring to ensure subjects can be held accountable.
      6. Authentication Factors Overview:
         1. Something you know (type 1 authentication factor): like password, PIN, or passphrase.
            1. Authoritative password recommendations:

NIST SP-800-63B, “Digital Identity Guidelines: Authentication and Lifecycle Management”

Password must be hashed

Passwords should not expire

Users should not be required to use special characters: NIST analyzed breached password databases and discovered that special characters in passwords didn’t provide the desired benefits.

Users should be able to copy and paste passwords.

Users should be able to use all characters

Password length should be at least eight characters and as many as 64 characters

Password systems should screen passwords

We occasionally visit government websites that requires passwords based on old advice. As an example, one government contracting website still includes the following rules:

1. Password expire after 60 days
2. Password must be at least 15 characters
3. Password must contain at least one uppercase letter
4. Passwords must contain at least one lowercase letter
5. Passwords must contain at least one number
6. Passwords must contain at least one special character.

Payment Card Industry Data Security Standards (PCI DSS) version 3.2.1

Password expire at least every 90 days.

Passwords must be at least seven characters long

* + - 1. Something you have (type 2 authentication factor): smartcard, hardware token, memory card, or USB drive.
         1. Smartcard (credit card-size ID or badge): has an integrated circuit chip embedded in it. It’s tamper-resistant and provide users with an easy way to carry and use complex encryption keys.
         2. Tokens (token device or hardware token): password-generating device that user can carry with them. Common token used today includes a display that shows a six- to eight-digit number. An authentication server stores the details of the token, so at any moment, the server knows what number is displayed on the user’s token. It uses dynamic OTP (onetime passwords).

Synchronous Dynamic Password Tokens: They generate a new PIN periodically, such as every 60 seconds, requiring the token and the server to have accurate time. A common way this is used is by requiring the user to enter a username, a static password, and the PIN into a web page. Other times, the system prompts users to enter the PIN after first entering their username and password.

Asynchronous Dynamic Password Tokens: generates PINs based on an algorithm and an incrementing counter.

Hardware tokens do have failings. If the battery dies or the device breaks, the user won’t be able to gain access. Some provide the PIN via a software application running on the user’s device (**Symantec** for example).

* + - 1. Something you are: fingerprints, face scans, retina patterns, iris paterns, and palm scans (biometric factors).
         1. False Rejection Rate, FRR (type I error)
         2. False Acceptance Rate, FAR (type II error)
         3. Crossover error rate, CER (or equal error rate ERR): the point where the FRR and FAR percentages are equal. Lower CERs means higher accuracy.

Biometric devices can be ineffective or unacceptable due to factors known as enrollment time, throughput rate, and acceptance. During enrollment, a subject’s biometric factor is sampled and stored in the device’s database. These stored sample is known as **reference profile** (or reference template).

In general, enrollment times over 2 minutes are unacceptable. Also, user may enroll again at regular intervals, adding inconvenience.

* + 1. Addition to authentication factors above, we also have:
       1. Somewhere you are: geographic location identified by an IP address or a phone number identified by Caller ID.
       2. Context-Aware Authentication: many MDM systems use this. If the user meets all the requirements (location, time, and type of device in this example), it allows the user to log on using the other methods, such as with a username and password.
    2. Multifactor Authentication: must be different factors (password and a PIN is not multifactor authentication because both are from a single authentication factor) used to authenticate at the same time.
    3. Two-Factor Authentication (2FA) with Authenticator Apps: for example, Microsoft Authenticator or Google Authenticator. Consider this context: You open Google Authenticator on your smartphone and see a six-digit PIN displayed. After entering the six-digit PIN, you have access. In this scenario, your smartphone is effectively mimicking a hardware token, making this two-factor authentication, though many organizations such as Google call it two-step authentication. This process typically takes advantage of the following standards:
       1. HOTP: HMAC-based OTP. It’s similar to the asynchrounous dynamic passwords created by tokens. The HOTP value remains valid until used.
       2. TOTP: The Time-based OTP. It uses timestamp and remains valid for a certain time frame. It’s similar to the synchronous dynamic passwords used by tokens.
    4. NIST Deprecates SMS for 2FA: the method of using SMS to send users a text with the PIN has a problem (but still better than just using a password). NIST SP 800-63B has pointed out several vulnerabilities with using SMS for two-step authentication and deprecated its use for federal agencies.
       1. If an attacker stole the smartphone or tablet, they would have access to the PIN
       2. Attacker may be able to convince a mobile operator to redirect SMS messages to an attacker’s devices (possible via SIM card fraud). If successful, attackers may be able to intercept SMS messages.
    5. Password Authentication: static passwords are the weakest form of authentication. Worse, as IT departments attempt to force users into creating longer and more complex passwords with expiration dates, users engage in risky behavior like writing down their passwords or creating weaker passwords. **Passwordless** authentication allows users to log into systems without entering a password.
       1. Fast Identity Online (FIDO) Alliance: an open industry association with a stated mission of reducing the over-reliance on passwords. They have created recommended frameworks and protocol standards: the FIDO2 project (now known as Web Authentication or WebAuthn) and the World Wide Web Consortium (W3C). Some of the problems they’ve identified with passwords are these:
          1. Users have as many as 90 online accounts
          2. Up to 51 percent of passwords are reused
          3. Passwords are the root cause of over 80 percent of data breaches
          4. Users abandon one-third of online purchases due to forgotten passwords
    6. Device Authentication: More and more employees are bringing their own mobile devices to work and hooking them up to the network. These devices aren’t necessarily able to join a domain, but it’s possible to implement device identification and authentication methods.
       1. Device fingerprinting: Users can register their devices with the organization and associate them with their user accounts. The device authentication system then captures the characteristics of the device (often accomplished by having the user access a web page with the device). The registration system then identifies the device using attributes such as the operating system and version, web browser, browser fonts, browser plug-ins (extensions), time zone, data storage, screen resolution, cookie settings, and HTTP headers. Even though some of these characteristics change over time, this has proven to be a successful device authentication method. Organizations often use third-party tools like SecureAuth Identity Provider (IdP). MDM systems use contexts-aware authentication methods to identify devices. **802.1X** is another method used for device authentication (implemented by MDM or NAC solutions).
    7. Service Authentication:
       1. Many services require authentication. A service account is simply a user account that an administrator created for a service or application instead of a person.
          1. It’s common to create a service account for third-party tools monitoring email in Microsoft’s Exchange Server. These third-party tools typically need permission to scan all mailboxes looking for spam, malware, potential data exfiltration attempts, and more.
          2. Service account has a high level of privileges, administrators configure it with a strong, complex password that is changed more often than regular users. However, administrators need to change these passwords manually. Another option is to configure the account to be noninteractive, which prevents a user from logging onto the account using traditional logon methods.
          3. Services can be configured to use certificate-based authentication (issued to the device running the service and presented by the service when accessing resources. Web-based services often use API methods to exchange information between systems. These API methods are different depending on the web-based service.
    8. Mutual Authentication: When a client access a server, both the client and the server provide authentication. Another example is when employees are connecting to a company network while working from home, they typically connect to a VPN server.

1. Implementing Identity Mangement (IdM): IdM techniques generally fall into two categories:
   1. Centralized access control: a single entity within a system performs all authorization verification. A small team or individual can manage centralized access control. They can scale up to support more users. However, it creates a **single point of failure**. Microsoft Active Directory is one example.
   2. Decentralized access control (also known as distributed access control): various entities located throughout a system perform authorization verification. It requires multiple teams or individuals and higher **administrative overhead** (day-to-day cost services without real productivity). Changes made to any individual access control point need to be repeated at every access point. Maintenance becomes difficult.
   3. SSO: a centralized access control technique. It’s convenient for users but it also has security benefits: users don’t have to remember multiple usernames and passwords, and users are less likely to write down a single password. SSO also eases administration by reducing the number of accounts required for a subject. However, once an account is compromised, an attacker gains unrestricted access to all of the authorized resources. Most SSO systems include methods to protect user credentials:
      1. LDAP and Centralized Access Control: a directory service is a centralized database that include information about subjects and objects. Many directory services are based on the Lightweight Directory Access Protocol (LDAP). For example, the Microsoft Active Directory Domain Services (AD DS) is LDAP based. You can think of an LDAP directory as a telephone directory for network services and assets. Users, clients, and processes can search the directory service to find where a desired system or resource resides. Subjects must authenticate to the directory service before performing queries and lookup activities. Even after authentication, the directory service will reveal only certain information to a subject, based on its assigned privileges. Multiple domains and trusts are commonly used in access control systems. A security domain is a collection of subjects and objects that share a common security policy, and individual domains can operate separately from other domains. **Trusts** are established between the domains to create a security bridge and allow users from one domain to access another domain’s resources. Trusts can be one-way only, or they can be two-way.
      2. LDAP and PKIs: A public key infrastructure (PKI) uses LDAP when integrating digital certificates into transmissions. There are many times when clients need to query a certificate authority (CA) for information on a certificate, and LDAP is one of the protocols used. LDAP and centralized access control systems can be used to support SSO capabilities.
      3. SSO and Federated Identities: Cloud-based applications use federated identity management (FIM) systems, which are a form of SSO. A federated identity links a user’s identity in one system with multiple identity management systems.
         1. FIM extends this beyond a single organization. Multiple organizations can join a federation or group, where they agree to share identity information. They can use this federated identity to access resources in any other organization within the group.
         2. A federation can be composed of multiple networks within a single university campus, numerous college and university campuses, multiple organizations sharing resources, or any other group that can agree on a common federated identity management system.
         3. Each organization decides what resources to share. Administrators manage these details behind the scenes, and the process is usually transparent to users. The important point is that users don’t need to enter their credentials again.
         4. A challenge with multiple companies communicating in a federation is finding a common language. Chapter 14 discusses the methods used to implement federated identity management systems. These include Security Assertion Markup Language (SAML), OAuth, and OpenID Connect (OIDC).
         5. Cloud-Based Federation: typically uses a third-party service to share federated identities. As an example, many corporate online training websites use federated SSO systems. When the organization coordinates with the online training company for employee access, they also coordinate the federated access details. A common method is to match the user’s internal login ID with a federated identity. Users log on within the organization using their normal login ID. When the user accesses the training website with a web browser, the federated identity management system uses their login ID to retrieve the matching federated identity. If it finds a match, it authorizes the user access to the web pages granted to the federated identity.
         6. On-Premise Federation: federated identity management systems can be hosted on-premises, in the cloud, or in a combination of the two as a hybrid system. Imagine Acme merges with Emca. Both companies have their own networks and SSO systems. However, management wants employees to be able to access resources in both networks without logging on twice. By creating an on-premises federated identity management system, both companies can share authentication data. This system allows users to continue to log on normally, but they will also have access to the other company’s network resources. An on-premises solution provides the organization with the most control.
         7. Hybrid Federation: a combination of a cloud-based solution and an on-premises solution. Imagine Acme has a cloud-based federation providing employees with online training. After the merger with Emca, they implement an on-premises solution to share identities with the two companies. This approach doesn’t automatically give employees from Emca access to the training sites. However, it’s possible to integrate the existing on-premises solution with the training sites’ cloud-based solution. This creates a hybrid solution for Emca employees and, as with other federated solutions, provides SSO for Emca employees.
         8. Just-in-time (JIT): Some federated identity solutions support JIT provisioning. These solutions automatically create the relationship between two entities so that new users can access resources. A JIT solution creates the connection without any administrator intervention. With JIT provisioning, employees log on normally to their employer’s network. The first time the employee accesses the benefits site, the JIT system exchanges data with the employer’s network and creates the employee’s account. JIT systems commonly use SAML to exchange the required data. SAML provides entities with a lot of flexibility to exchange a wide assortment of data. The process starts with the third party verifying the user is logged onto a trusted organization’s network. The employer’s network then sends data on the employee, such as the username, first and last name, email address, and any other information needed by the third party.
      4. Credential Management Systems: provide storage space for usernames and passwords. The W3C published the Credential Management Level 1 API as a working draft in January 2019. Many web browsers have adopted the API for credential management. The API provides several benefits that developers can implement **programmatically**:
         1. Offering to store the user’s credentials after logging on
         2. Showing an account chooser, allowing the user to skip forms
         3. Automatically logging the user on in subsequent visits, even if the session has expired.

Some federated identity management use the Credential Management API, allowing different web applications to implement SSO solutions using a federated identity provider (like you can use Google or Facebook account to sign in to Zoom).

Identity as a service, or identity and access as a service (IDaaS), is a third-party service that provides identity and access management. IDaaS effectively provides SSO for the cloud and is especially useful when internal clients access cloud-based software as a service (SaaS). Users log into their Google account once, and it provides them access to multiple Google cloud-based applications without requiring users to log in again. For example, Office 365 provides Office applications as a combination of installed applications and SaaS applications. Users have full Office applications installed on their user systems, which can also connect to cloud storage using OneDrive. This allows users to edit and share files from multiple devices. When people use Office 365 at home, Microsoft provides IDaaS, allowing users to authenticate via the cloud to access their data on OneDrive. When employees use Office 365 from within an enterprise, administrators can integrate the network with a third-party service. For example, Centrify provides third-party IDaaS services that integrate with Microsoft Active Directory. Once configured, users log onto the domain and access Office 365 cloud resources without logging on again.

* + 1. Credential Manager Apps:
       1. Windows includes the Credential Manager applet in the Control Panel. When a user enters credentials in a browser or a Windows application, it offers to save them. It encrypts the credentials and stores them.
       2. Third-party credential manager systems: For example, KeePass is a freeware tool that allows you to store your credentials. Credentials are stored in an encrypted database, and users can unlock the database with a master password. Once it’s unlocked, users can copy their passwords and paste.
    2. Scripted Access (or logon scripts): establish communication links by providing an automated process to transmit login credentials at the start of a login session.
       1. It often simulate SSO even though the environment still requires a unique authentication process to connect to each server or resource.
       2. Scripts can implement SSO in environments where true SSO technologies are not available.
       3. Scripts and batch files should be stored in a protected area because they usually contain access credentials in cleartext.
    3. Session Management: it’s important to use session management methods to prevent unauthorized access, including sessions on regular computers such as desktop PCs and within online sessions with an application.
       1. Desktop PCs and laptops include screen savers (changing the display when the computer isn’t in use by displaying random patterns or different pictures or simply blanking the screen). They have a password-protect feature that can be enabled. This feature displays the logon screen and forces the user to authenticate again before exiting the screen saver.
       2. Secure online sessions will typically terminate after sometime too (like many bank account website does).
       3. The OWASP publishes many different “cheat sheets” that provide application developers’ specific recommendations. The **Session Management Cheat Sheet** provides information about web sessions and various methods used to secure them.
       4. Developers commonly use web development frameworks to implement session management. This identifier is include in every HTTP request throughout the session. These also include methods to expire sessions. High-value applications such as applications accessing financial data typically have timeout ranges of 2 to 5 minutes. Low-value applications typically have timeout ranges of 15 to 20 minutes.

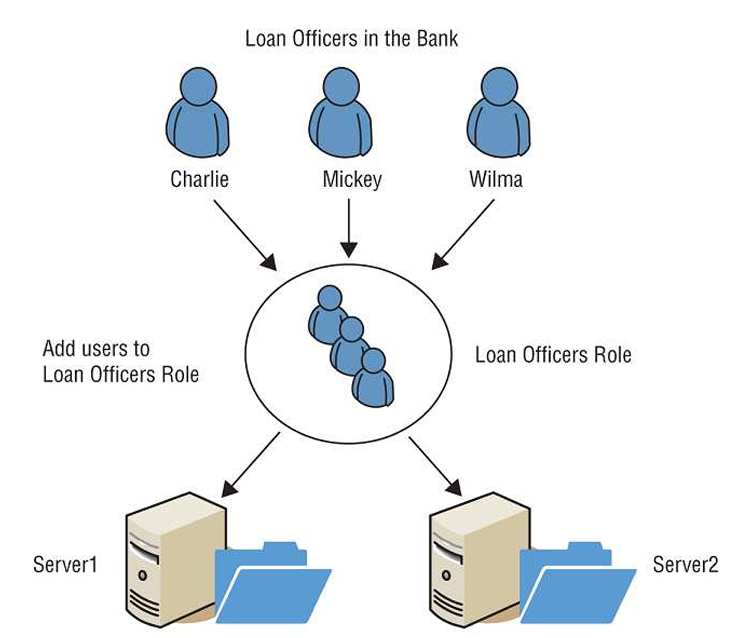
1. Managing the Identity and Access Provisioning Lifecycle
   1. Provisioning and Onboarding
      1. Automated provisioning systems: create accounts consistently, such as always creating usernames the same way and treatng duplicate usernames consistently.
      2. Provisioning also includes issuing hardware such as laptops, mobile devices, hardware tokens, and smartcards to employees. It’s important to have accurate records.
      3. Onboarding process include items such as the following:
         1. Having them read and sign the AUP
         2. Explaining security best practices, such as how to avoid infections from emails.
         3. Reviewing the organization’s mobile device policy, if applicable
         4. Ensuring that the employee’s computer is operational and that the employee can log on
         5. Helping the employee configure a password manager, if available
         6. Assisting the employee with configuring 2FA, if available
         7. Explaining how to access help desk personnel for further assistance
         8. Showing the employee how to access, share, and save resources

Some seems unnecessary. Consider an organization that uses nonpersistent virtual desktops. When the user logs off, all data and settings are lost. A new employee can spend a day creating and saving files, only to come bck the next day and find that everthing is gone.

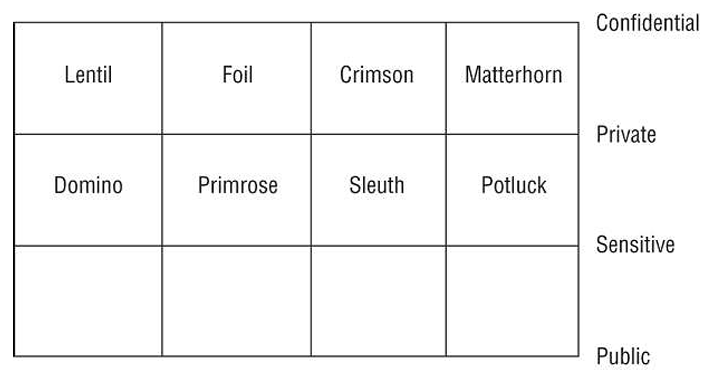
* 1. Deprovisioning and Offboarding
     1. The easiest way to deprovision an account is to delete it (account revocation). However, it may remove access to the user’s data (like when the user’s data is encrypted).
     2. Disable the account: supervisors can review the user’s data and determine if anything is needed before deleting the account. Adminstrators can change the user’s password and give the supervisor the new password. Organizations typically have policies in place to delete these disabled accounts within 30 days (can be varied).
     3. If a terminated employee retains access to a user account after the exit interview, the risk of sabotage is very high. Other employees may be able to use the account.
     4. It’s also important to terminate employee benefits as part of the offboarding process.
  2. Defining New Roles: imagine an organization decides to start selling items with an e-commerce site hosted on a new Linux server running Apache. Developers will write and maintain the code for the site, and administrators will manage the server. If they don’t already have website developers and Linux administrators, they may decide to create two new roles to support this project. They would also define the privileges needed for these new roles and how they plan on assigning the privileges, such as with groups.
  3. Account Maintenance:
     1. organizations with static organizational hierarchies and low employee turnover or promotion will conduct significantly less account administration than an organization with a flexible or dynamic organizational hierarchy and high employee turnover and promotion rates.
     2. Most account maintenance deals with altering rights and privileges. Procedures similar to those used when creating new accounts should be established to govern how access is changed throughout the life of a user account.
  4. Account Access Review
     1. Check to ensure accounts comply with security policies. The “Device Authentication” section in this chapter discussed system accounts, such as those assigned to computers, and the “Service Authentication” section in this chapter discussed service accounts.
     2. The local system account on computers typically has the same privileges as the local administrator account, allowing the computer to access other computers on the network as the computer, instead of as a user. Some applications use the local system as the service account, allowing to run without creating a special service account, but it often grants the application more access than it needs. If an attacker exploits an application vulnerability, the attacker may gain access to the service account.
     3. Many administrators use scripts to check for inactive accounts periodically (and automatically disable them). Similarly, scripts can check group membership of privileged groups (such as administrator groups) and remove unauthorized accounts. Routine auditing procedures often include account reviews.
     4. Privilege monitoring audits accounts: have elevated privileges. This include accounts with administrator privileges like administrator accounts, root accounts, service accounts, or any that has more privileges than a regular user.
     5. Two problems related to access control:
        1. Excessive privilege
        2. Creeping privilege (or privilege creep): involves a user account accumulating additional privileges over time as job roles and assigned tasks change.

Chapter 14

1. Comparing Access Control Model
   1. Comparing Permissions, Rights, and Privileges
      1. Permissions: the access granted for an object and determine what you can do with it
      2. Rights: ability to take an action on an object
      3. Privileges: combination of rights and permissions
   2. Understanding Authorization Mechanism
      1. Implicit Deny: access to an object is denied unless access has been explicitly granted to a subject.
      2. Access Control Matrix: a table that includes subjects, objects, and assigned privileges. An access control matrix can include a group of files as the objects and a group of users as the subjects. This covers much more than a single access control list (ACL). Each file listed within the matrix has a separate ACL that lists the authorized users and their assigned permissions.
      3. Capability Tables: different from ACLs in that a capability table is focused on subjects (like users, groups, or roles). It helps identify privileges assigned to subjects.
      4. Constrained Interface (or restricted interface): Applications use constrained interfaces to restrict what users can do or see based on their privileges. The Clark-Wilson model discusses the technical details of how it implements a constrained interface.
      5. Content-Dependent Control: restrict access to data based on the content within an object. A database view (like in SQL query) is a content-dependent control.
      6. Context-Dependent Control: require specific activity before granting users access (like when you purchasing on the website that leads to different distinct pages). It’s also possible to use date and time controls as context-dependent controls (like denying access when the user access outside the allowed time).
      7. Need to Know: subjects are granted minimum accesses
      8. Least Privilege: subjects are granted minimum privileges.
      9. Separation of Duties and Responsibilities: helps prevent fraud and errors by creating a system of checks and balances.
   3. Defining Requirements with a Security Policy: security policy defines security requirements for an organization. Some organizations create multiple security policies focusing on a separate area. It may state the need to implement and enforce separation of duties and least privilege principles but not state how to do so.
   4. Introducing Access Control Models:
      1. Discretionary Access Control: every object has an owner (data custodian and the owner can grant or deny access to any other subjects. The New Technology File System (NTFS), used on Microsoft Windows operating systems, uses the DAC model.
      2. Role-Based Access Control:
         1. Instead of assigning permissions directly to users, user account are placed in roles and administrators assign privileges to the roles. These roles are typically identified by job functions.
         2. Examples: Microsoft Windows operating systems implement this model with the use of groups. A bank may have loan officers, tellers, and managers. Administrators can create a group named Loan Officers, place the user accounts of teach loan officer into this group, and then assign appropriate privileges to the group. If the organization hires a new loan officer, administrators simply add the new loan officer’s account into the Loan Officers group, and the new employee automatically has all the same permissions as other loan officers in this group. Administrators would take similar steps for tellers and managers.
         3. Administrators often implement RBAC using groups. This approach helps enforce the principle of least privilege by preventing privilege creep. Ideally, administrators revoke user privileges when users change jobs within an organization.
         4. Another method related to RBAC is task-based access control. Instead of being assigned to one or more roles, each user is assigned an array of tasks. The focus is on controlling access by assigned tasks rather than by user identity. Microsoft Project uses TBAC. Each project has multiple tasks. The project manager assigns tasks to project team personnel. Team personnel can address their own tasks (adding comments, indicating progress, and so on), but they cannot address other tasks. Microsoft Project handles the underlying details.



* + 1. Rule-Based Access Control: it applies global rules to all subjects. A firewall uses rules that allow or block traffic to all users equally. Rules within the rule-based access control model are sometimes referred to as restrictions or filters.
    2. Attribute-Based Access Control: its use of rules that can include multiple attributes, allowing it to be much more flexible than a rule-based access control model that applies the rules to all subjects equally. It’s an advanced implementation of a rule-based access control. Many SDNs use the ABAC model. Additionally, ABAC allows administrators to create rules within a policy using plain language statements such as “Allow Managers to access the WAN using a mobile device.” MDM systems can use attributes to identify mobile devices, allowing the user to log on when the attributes match and verified.
    3. Mandatory Access Control: the use of labels is applied to both subjects and objects. If a user has a label of top secret, the user can be granted access to a top-secret document (matching labels). When documented in a table, the MAC model sometimes resembles a lattice (such as the one used for a climbing rosebush), so it is referred to as a lattice-based model. For the example below, within the Confidential section (Lentil, Foil, Crimson, and Matterhorn), users also require the additional label to access data within these compartments. To access Lentil data, users need to have both the Confidential label and the Lentil label. Notice that Sensitive data doesn’t have any additional labels. Users with the Sensitive label can be granted access to any data with the Sensitive label. Using compartmentalization with the MAC model enforces the *need to know* principle. The MAC model is more security than the DAC model, but it isn’t as flexible or scalable. Classifications within a MAC model use one of the following three types of environment:
       1. Hierarchical Environment: relates various classification labels in an ordered structure from low security to medium security to high security (like Confidential, Secret, and Top Secret). Clearance in one level grants the subject access to objects in that level as well as to all objects in lower levels.
       2. Compartmentalized Environment: there’s no relationship between one security domain and another. To gain access to an object, the subject must have specific clearance for the object’s security domain.
       3. Hybrid Environment: Combining both hierarchical and compartmentalized concepts so that each hierarchical level may contain numerous subdivisions that are isolated from the rest of the security domain. It provides granular control over access but becomes increasingly difficult to manage as it grows.



* + 1. Risk-Based Access Control: grants access after evaluating risk. It evaluates the environment and the situation and makes risk-based decisions using policies embedded within software code. It uses machine learning to make predictive conclusions about current activity based on past activity. Or, it can sometimes use binary rules to control access. Consider this scenario: an information system containing patient information and used by medical professionals. Doctors, nurses, and others working in the emergency room (ER) of a hospital need access to this data for any patient who shows up in the ER. The model attempts to evaluate risk by considering several different elements, such as:
       1. The environment: is the ER in this example. Within cybersecurity, the environment can include items such as the location using the IP address. Some low-risk IP addresses may internal IP addresses and internet-based IP addresses of users who have previously signed in. High-risk IP addresses could be from foreign coutnries, anonymized IP addresses, users signed in from two or more IPs in different countries, and users signed in from unfamiliar locations.
       2. The situation: is the medical emergency in this example. Moreover, the situation may include what a device is doing. Most IoT devices have predictable behavior. If an IoT device suddenly starts flooding a network with malicious traffic, the risk-based model could determine the device is now a high risk and block its access to a network.
       3. Security policies: software code that makes risk-based decisions based on available data. An organization would modify the choices within the software to support their needs. In this example, it consider this a low risk and grant full access to patient data to doctors and nurses.
       4. Two other things can be checked or required before the policy grants access:
          1. Multifactor Authentication
          2. Compliant Mobile Devices: the policy may require that smartphones and tablets meet specific security requirements.
  1. Discretionary Access Control with some subsets: Data owners can also delegate day-to-day tasks for handling data to data custodians, giving data custodians the ability to modify permissions. A DAC model is implemeneted using ACLs on objects. Each ACL defines the types of access granted or denied to subjects. It doesn’t offer a centrally controlled management system because owners can alter the ACLs on their objects at will.
     1. Identity-based access control: systems identify users based on their identity and assign resource ownership to identities
  2. Nondiscretionary Access Control: Administrators centrally administer nondiscretionary access controls and can make changes that affect the entire environment. Access doesn’t focus on user identity. Instead, a static set of rules governing the whole environment manage access. Non-DAC systems are centrally controlled and easier to manage (although less flexible). In general, any model that isn’t a discretionary model is a nondiscretionary model.

1. Implementing Authentication Systems: FIM allows different organizations to use federations for SSO.
   1. Implementing SSO on the Internet: Imagine you want to transfer money from Bank A to Bank B. You could give Bank B your credentails to Bank A and have them transfer the money. Sound scary? You bet. You should never be required to give your credentials to any third party. Solutions such as SAML, OAuth, OpenID, and OIDC help solve this problem. They share authentication, authorization, or profile information about a user, and some solutions share all three.
      1. XML: databases from multiple vendors can import and export data to and from an XML format, making XML a common language used to exchange information if companies agree on what **schema** to use. Many cloud-based providers use XML-based languages to share information for authentication and authorization. They don’t use XML as it is but instead use other languages based on XML.
      2. SAML: an open XML-based standard commonly used to **exchange authentication and authorization (AA) information** between federated organizations. It **provides SSO capabilities** for browser access. The Organization for the Advancement of Structured Information Standards (OASIS), a nonprofit consortium that encourages open standards development, adopted SAML 2.0 (a convergence of SAML 1.1, the Liberty Alliance Identity Federation Framework, ID-FF, 1.2, and Shibboleth 1.3) as an OASIS standard in 2005 and has maintained it since then. (www.oasis-open.org/standards) site has more details on SAML 2.0. Example: imagine Sally is accessing her investment account at ucanbeamillionaire.com that requires her to log on to access her acocunt, and the site uses SAML:
         1. Principal or User Agent: think of Sally as the principal who’s trying to access her investment account at ucanbeamillionaire.com
         2. Service Provider (SP): ucanbeamillionaire.com site is providing the service
         3. Identity Provider (IdP): This is a third party that holds the user authentication and authorization information. It can send three types of XML messages known as assertions:
            1. Authentication Assertion: provides proof that the user agent provided the proper credentials, identifies the identification method, and identifies the times the user agent logged on.
            2. Authorization Assertion: indicates whether the user agent is authorized to access the requested service. If the message indicates access is denied, it indicates why.
            3. Attribute Assertion: can be any information about the user agent.
      3. OAuth (OAuth 2.0 implying open authorization): an authorization framework described in RFC 6749 and maintained by the Internet Engineering Task Force (IETF). Many companies on the internet use it to share account information with third-party websites.
         1. Example: imagine you have a Twitter account, and you download an app called Acme that can interact with your Twitter account and schedule Tweets in advance. When you try to use the feature in the Acme app, it redirects you to Twitter. Twitter propts you to log on, shows you what permissions the Acme app will access, and then asks if you want to authorize the Acme app to access your Twitter app. If you approve, Twitter sends the Acme app an authorization token. The app may accept and enter the authorization token directly, or you may need to enter it into the app’s settings. When the app accesses the Twitter account, it sends an API message and includes the token. Note that this doesn’t provide authentication. Instead, it authorizes access to the account. A primary benefit is that you never provide your Twitter credentials to the Acme app. Even if the Acme app is compromised, it does not expose your credentials.
         2. Note: OAuth 2.0 is note backward compatible with OAuth 1.0. OAuth is an authorization framework, not an authentication protocol. It exchanges API messages and uses a token to show that access is authorized.
      4. OpenID: provides decentralized authentication, allowing users to log into multiple unrelated websites with one set of credentials maintained by a third-party service (referred to as an OpenID provider). It’s an open standard but it’s maintained by the OpenID Foundation rather than as an RFC standard.
         1. Explanation: when users go to an OpenID-enabled website (also known as a relying party), they are prompted to provide their OpenID identity as a URI. The OpenID-enabled website and an OpenID provider exchange data and create a secure channel. The user is then redirected to the OpenID provider and is prompted to provide the password. If correct, the user is redirected back to the OpenID-enabled site (check this [site](openidexplained.com/use) to see how this works).
         2. Example: if your OpenID identifier is bobsmith2021.myopenid.com, that’s what you have to enter. In contrast, other methods exchange data behind the scenes, so it isn’t as obvious what method is being used.
         3. OIDC (OpenID Connect): an authentication layer using the OAuth 2.0 authorization framework. It’s maintained by the OpenID Foundation. It builds on the technologies created with OpenID but uses a JWT (or ID token). OIDC uses a web service to retrieve the JWT. In addition to providing authentication, the JWT can also include profile information about the user. Practice on understanding JWT: this [practice](https://play.picoctf.org/practice/challenge/236?category=1&page=4) can help you gain more understanding about JWT (also where I first learned about it). Example: Most of this occurs behind the scenes, but you can see it in action by logging onto eBay with a Google account. These processes and interfaces change over time, but the general steps are as follows:
            1. If you don’t have a Google account, create one first.
            2. Ensure you’re logged out of eBay and Google, go to ebay.com, and click Sign In.
            3. Click Continue With Google. A dialog box opens, prompting you to enter your Google email. It also indicates what Google will share with ebay.com.
            4. Enter your email address and press Enter.
            5. Enter your password and click Next.
            6. If you’ve enabled 2-Step Verification on your Google account, you’ll be prompted to get the code and enter it.
            7. You don’t need to complete the creation of an eBay account with your Google account. However, if you choose to do so, click the Create Account button. You’ll now be logged on to eBay using your Google account. If you log out of eBay and try to log on again, all you need to do is click Sign In and then click Continue with Google. As long as you’re still logged on with Google, you’ll be logged in to eBay without any more steps.
   2. Comparing SAML, OAuth, OpenID, and OIDC
      1. SAML:
         1. SAML 2.0 is an open XML-based standard
         2. OASIS adopted it as a standard in 2005
         3. It utilizes three entities: a principal (such as a user), a service provider (such as a website), and an identity provider (a third party that holds the authentication and authorization information)
         4. It can provide authentication, authorization, and attribute information on the principal
      2. OAuth:
         1. It’s an authorization framework, not an authentication protocol
         2. RFC 6749 describes OAuth 2.0
         3. It exchanges information using APIs
         4. An app obtains an access token from an identity provider
         5. Later, the app includes the access token for authorization
      3. OpenID
         1. OpenID is an authentication standard
         2. It is maintained by the OpenID Foundation
         3. An OpenID provider provides decentralized authentication
         4. Users enter their Open ID identifier (such as bobsmith2021.myopenid.com) on a site and the OpenID provider verifies the identifier.
      4. OIDC
         1. OIDC is an authentication layer using OAuth 2.0
         2. It builds on the OpenID authentication standard
         3. It provides both authentication and authorization
         4. It builds on OpenID but uses a JWT.
   3. Implementing SSO on Internal Networks: Network access methods allow users to access internal networks from remote locations (such as at home). Kerberos is the most common. Two common remote access protocols are RADIUS and TACACS+. In addition to supporting SSO, RADIUS and TACS+ provider authentication, authorization, and account.
      1. AAA Protocols (authentication, authorization, and accounting): provide centralized access control with remote access systems such as VPNs. They help protect internal LAN authentication systems and other servers from remote attacks.
         1. Example: If you are using a separate system for remote access, a successful attack on the system only affects the remote access users. Attacker won’t have access to internal accounts. They ensure that users have valid credentials to authenticate and verify that they are authorized to connect to the remote access server based on the user’s proven identity.
         2. Additionally, the accounting element can track the user’s network resource usage, which can be used for billing purposes.
      2. Kerberos: an important authentication system to know for the CISSP exam and a well-known ticket system.
         1. Ticket authentication: a mechanism that employs a third-party entity to prove identification and provide authentication.
         2. Primary purpose of Kerberos: authentication. Keberos uses users’ proven identity to issue tickets, and user accounts present these tickets when access resources.
         3. Offering a SSO solution for users and protect logon credentials.
         4. Kerberos verions 5 relies on symmetric-key cryptography (secret-key cryptography) using AES. Kerberos provides confidentiality and integrity for authentication traffic using end-to-end security and helps protect against eavesdropping and replay attacks.
         5. Many of Kerberos roles are on a single server, but they can be installed on different servers. Larger networks sometimes separate them to increase performance, but small networks typically have one kerberos server performing all of the different roles.
         6. List of important elements used in Kerberos:
            1. Key Distribution Center: the trusted third party that provides authentication services. Kerberos uses symmetric-key cryptography to authenticate clients to servers. All clients and servers are registered with the KDC, and it maintains the secret keys for all network members.
            2. Kerberos Authentication Server: the authentication server hosts the functions of the KDC: a ticket-granting service (TGS) and an authentication service (AS). However, it’s possible to host the ticket-granting service on another server. The AS verifies or rejects the authenticity and timeliness of tickets. This server is often called the KDC.
            3. Ticket (sometimes called server ticket, ST): an encrypted message that provides proof that a subject is authorized to access an object. Subjects (like users) request tickets to access objects (such as files), and if they have authenticated and are authorized to access the object, Kerberos issues them a ticket (having specific lifetimes and usage parameters). If the ticket expires, a client must request a renewal or a new ticket.
            4. Ticket-Granting Ticket (TGT): provides proof that a subject has authenticated through a KDC and is authorized to request tickets to access other objects. A TGT is encrypted and includes a symmetric key, an expiration time, and the user’s IP address.
            5. Kerberos Principal: Kerberos issues tickets to Kerberos principals. A Kerberos principal is typically a user but can be any entity that can request a ticket.
            6. Kerberos Realm: a logical area controlled or ruled by Kerberos. Principals within the realm can request tickets from Kerberos, and Kerberos can issue tickets to principals in the realm.
         7. The database of accounts could be stored in a directory service such as Microsoft’s Active Directory (AD), which enables Kerberos by default.
         8. The Kerberos login process works as follows:
            1. The user types a username and password into the client
            2. The client generates a request with these credentials to the KDC. This request transmission is encrypted
            3. The KDC verifies the username against its database of known credentials
            4. The KDC generates a session key that will be used by the client and the Kerberos server. It encrypts this with a hash of the user’s password. The KDC also generates an encrypted timestamped TGT.
            5. The KDC then transmits the encrypted session key and the encrypted timestamped TGT to the client.
            6. The client installs the TGT for use until it expires. The client also decrypts the session key using a hash of the user’s password.
         9. When a client wants to access an object, it must request a ticket through the Kerberos server:
            1. The client sends its TGT back to the KDC with a request for access to the resource.
            2. The KDC verifies that the TGT is valid and checks its access control matrix to verify that the user has sufficient privileges to access the requested resource.
            3. The KDC generates a service ticket and sends it to the client.
            4. The client sends the ticket to the server or service hosting the resource.
            5. The server or service hosting the resource verifies the validity of the ticket with the KDC.
            6. Once identity and authorization are verified, Kerberos activity is complete. The server or service host then opens a session with the client and begins communications or data transmission.
         10. Kerberos is a versatile authentication mechanism that works over local LANs, remote access, and client/server resource requests. However, it presents a single point of failure (the KDC). If the KDC is compromised, the secret for every system on the network is also compromised. If a KDC goes offline, no subject authentication can occur.
         11. It also has strict time requirements, and the default configuration requires that all systems be time-synchronized within 5 minutes of each other. Administrators often configure a time synchronization system within a network. In an Active Directory domain, one domain controller (DC) synchronizes its time with an external Network Time Protocol (NTP) server. All other DCs synchronize their time with the first DC. All other systems synchronize their time with one of the DCs when they log on.
      3. RADIUS (Remote Authentication Dial-in User Service): centralizes authentication for remote access connections (like with VPNs or dial-up access).
         1. It’s typically used when an organization has more than one **network access server** (or remote access server). A user can connect to any network access server, which then passes on the user’s credentials to the RADIUS server to verify authentication and authorization and to track accounting. In this context, the network access server is the RADIUS client, and a RADIUS server acts as an authentication server.
         2. Many internet service providers (ISPs) use RADIUS for authentication. User can access the ISP from anywhere, and the ISP server then forwards the user’s connection request to the RADIUS server.
         3. Organizations can also use RADIUS, and organizations often implement it with location-based security. Althought it itsn’t as common today, some users still have Integrated Services Digital Network (ISDN) dial-up lines and use them to connect to VPNs. Users call in, and after authentication, the RADIUS server terminates the connection and initiates a call back to the user’s predefined phone number.
         4. RADIUS uses the UDP by default and encrypts only the password’s exchange. RADIUS can use other protocols to encrypt the data session. The current version is defined in RFC 2865. RFC 6614, designated as Experimental, defines how RADIUS can use TLS over TCP. When using TLS, RADIUS uses TCP port 2083. RADIUS uses UDP port 1812 for RADIUS messages and UDP port 1813 for RADIUS Accounting message. Interestingly, an early draft of RADIUS/TLS was called TLS encryption for RADIUS over TCP (RadSec). However, RFC 6614 omitted the parenthetical RadSec. Radiator Software still sells Radiator and refers to RadSec as “secure, reliable RADIUS proxying.” However, it’s also possible to use RADIUS/TLS to encrypt the entire session.
      4. TACACS+ (Terminal Access Controller Access Control System Plus): provides several improvements over the earlier versions and over RADIUS. It separates authentication, authorization, and accounting into separate processes, which can be hosted on three different servers if desired. Additionally, it encrypts all of the authentication information, not just the password, as RADIUS does. TACACS+ uses TCP port 49, providing a higher level of reliability for the packet transmissions.
2. Understanding Access Control Attacks
   1. Privilege escalation: The easiest way to do this is to use the LocalSystem account because it has full administrative privileges on the local system, and you don’t have to manage the password. However, the easiest way is not the correct way. Instead, you would create a new account and give it only the needed rights and permissions.
   2. Using the su and sudo commands
   3. Minimizing the Use of sudo
   4. Password Attacks
   5. Dictionary Attacks
   6. Brute-Force Attack
   7. Spraying Attack
   8. Credential Stuffing Attack
   9. Birthday Attack
   10. Rainbow Table Attack
   11. Mimikatz: Some capabilities of Mimikatz:
       1. Read passwords from Memory: Plaintext passwords and PINs stored in the Local Security Authority Subsystem Service (LSASS), which can be extracted and read.
       2. Extract Kerberos Tickets: Mimikatz includes Kerberos module that can access the Kerberos API.
       3. Extract Certificates and Private Keys: Mimikatz includes a Windows CrytoAPI module.
       4. Read LM and NTLM password hashes in memory: Some Windows systems still create LM hashes in the local Security Account Manager database and store it in memory. This can be prevented
       5. Read cleartext passwords in Local Security Authority Subsystem Service (LSASS): The LSASS doesn’t normally store passwords in cleartext, but malware can modify the registry to enable digest authentication.
       6. List running processes
   12. Pass-the-Hash (PtH) attack: For example, use a tool such as Mimikatz to capture user hashes stored in the lsass.exe process.
   13. Kerberos Exploitation Attack
       1. Overpass the Hash: an alternative to the PtH attack used when NTLM is disabled on a network.
       2. Pass the Ticket: attacker harvests tickets held in the lsass.exe process
       3. Silver Ticket: uses the captured NTLM hash of a service account to create a ticket-granting service (TGS) ticket.
       4. Golden Ticket: attackers can create tickets at will within AD by obtaining the hash of the Kerberos service account (KRBTGT)
       5. Kerberos Brute-Force: use the Python script kerbrute.py on Linux systems or Rubeus on Windows systems.
       6. ASREPRoast: identifies users that don’t have Kerberos preauthentication (a security feature within Kerberos that helps prevent password-guessing attacks) enabled. The KDC will reply with a TGT, encrypted with the client’s password as the key. The attacker can then perform an offline attack to decrypt the ticket.
       7. Kerberoasting: collects encrypted TGS tickets. Service accounts use TGS tickets instead of TGT tickets. Attackers then crack them offline. This attack attempts to find users that don’t have Kerberos preauthentication
   14. Sniffer Attack: To prevent:
       1. Controlling physical access to routers and switches prevents attackers from installing sniffers on these devices
       2. IDS can monitor the network for sniffers
   15. Spoofing attacks
       1. Email Spoofing: the Reply To field can be a different email address from the email address of the sender. It’s often ignored.
       2. Phone number spoofing: allows a caller to replace this number with another one, which is a common technique on VoIP systems.
3. Core Protection Methods
   1. Control physical access to systems
   2. Control electronic access to files
   3. Hash and salt passwords: helps prevent rainbow tables or other methods
   4. Use password masking
   5. Deploy multifactor authentication:
   6. Use account lockout controls: lock an account after the incorrect password is entered a predefinedn number of times. For systems and services that don’t support account lockout controls, such as most FTP servers, extensive logging along with an IDS can protect the server.
   7. Use last logon notification: helps users keep track of someone logging into their account
   8. Educate users about security

Domain 6:

1. Building a Security Assessment and Testing Program (Chapter 15)
   1. Security tests
      1. Availability of security testing resources
      2. Criticality of the systems and applications protected by the tested controls
      3. Sensitivity of information contained on tested systems and applications
      4. Likelihood of a technical failure of the mechanism implementing the control
      5. Likelihood of a misconfiguration of the control that would jeopardize security
      6. Risk that the system will come under attack
      7. Rate of change of the control configuration
      8. Other changes in the technical environment that may affect the control performance
      9. Difficulty and time required to perform a control test
      10. Impact of the test on normal business operations
      11. Note: many security testing programs begin on haphazard basis, with security professionals simply pointing their fancy new tools at whatever systems they come across first. Experimentation with new tools is fine, but security testing programs should be carefully designed and include rigorous, routine testing of systems using a risk-prioritized approach.
   2. Security assessments: comprehensive reviews of the security of a system, application, or other tested environment. It normally includes the use of security testing tools but go beyond automated scanning and manual penetration tests, including a thoughtful review of the threat environment, current and future risks, and the value of the targeted environment.
      1. NIST SP 800-53A: Assessing Security and Privacy Controls in Federal Inforamtion Systems and Organizations: Building Effective Assessment Plans (nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf)
         1. Specifications: the documents associated with the system being audited. Specifications generally include policies, procedures, requirements, specifications, and designs.
         2. Mechanisms: the controls used within an information system to meet the specifications. They can be based in hardware, software, or firmware
         3. Activities: actions (carried out by people within an information system) that may include performing backups, exporting log files, or reviewing account histories.
         4. Individuals: people who implement specifications, mechanisms, and activities
   3. Security audits: assessment and testing results are meant for internal use only. Audits provide an impartial, unbiased view of the state of security controls. The reports written by them are intended for different audiences (unlike assessment) that may include an organization’s board of directors, government regulators, and other third parties.
      1. Internal audits: In many organizations, the chief audit executive reports directly to the president (CEO or similar role). The chief audit executive (CAE) may also have reporting responsibility directly to the organization’s governing board.
      2. External audits: There are thousands of firms that perform external audits, but most large organizations use the so-called Big Four audit firms:
         1. Ernst & Young
         2. Deloitte
         3. PricewaterhouseCoopers
         4. KPMG
      3. Third-party audits: conducted by (or on behalf of) another organization. Organizations that provide services to other organizations are frequently asked to participate in third-party audits. This can be quite a burden on the audited organization if they have a large number of clients.
         1. The American Institue of Certified Public Accountants (AICPA) released a standard designed to alleviate this burden.
         2. The Statement on Standards for Attestation Engagements document 18 (SSAE 18), titled Reporting on Controls, provides a common standard to be used by auditors performing assessments of service organization with the intent of allowing the organization to conduct an external assessment instead of multiple third-party assessments and then sharing resulting report with customers and potential customers.
         3. Outside of the US, similar engagements are conducted under the Internation Standard for Attestation Engagements (ISAE) 3402, Assurance Reports on Controls at a Service Organization.
         4. SSAE 18 and ISAE 3402 engagements are commonly referred to as service organization controls (SOC) audits, and they come in three forms:
            1. SOC 1 Engagements: assess the organization’s controls that might impact the accuracy of financial reporting
            2. SOC 2 Engagements: assess the organization’s controls that affect the security (confidentiality, integrity, and availability) and privacy of information stored in a system. SOC 2 audit results are confidential and are normally only shared outside the organization under an NDA.
            3. SOC 3 Engagements: assess the organization’s controls that
         5. In addition to the three categories of SOC assessment, there are 2 different types of SOC report. Both reports begin with providing a description by management of the controls put in place. They differ in the scope of the opinion provided by the auditor:
            1. Type I Reports: provide the auditor’s opinion on the description provided by management and the suitability of the design of the controls. It also cover only a specific point in time, rather than an extended period. It’s more of a documentation review where the auditor is checking things out on paper and making sure that the controls described by management are reasonable and appropriate.
            2. Type II Reports: go further and also provide the auditor’s opinion on the operating on the operating effectiveness of the controls. The auditor actually confirms that the controls are functioning properly. The report also covers an extended period of time: at least six months of operation. It’s more like a traditional audit. It’s not just checking the paperwork; they are also going in and verifying that the controls function properly.
      4. Information security professionals are often asked to participate in internal, external, and third-party audits. Auditors may also request the participation of security staff members in the execution of control evaluations. Auditors generally have **carte blanche** access to all information within an organization, and security staff should comply with those requests, consulting with management as needed.
      5. Addition section: Government Auditors Discover Air Traffic Control Security Vulnerabilities: The U.S. Government Accountability Office (GAO) performs audits at the request of Congress, and these GAO audits often focus on information security risks. In 2015, the GAO released an audit report titled “Information Security: FAA Needs to Address Weaknesses in Air Traffic Control Systems.” This report’s conclusion was damning: “While the Federal Aviation Administration FAA has taken steps to protect its air traffic control systems from cyber-based and other threats, significant security control weaknesses remain, threatening the agency’s ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). These include weaknesses in contorls intended to prevent, limit and detect unauthorized access to computer resources, such as controls for protecting system boundaries, identifying and authenticating users, authorizing users to access systems, encrypting sensitive data, and auditing and monitoring activity on FAA’s systems.” The report went on to make **17 recommendations** on how the FA might improve its information security controls to better protect the integrity and availability of the nation’s air traffic control system (found in [www.gao.gov/assets/670/668169.pdf)](http://www.gao.gov/assets/670/668169.pdf))
      6. Auditing Standards: One common framework for conducting audits and assessments is the Control Objectives for Information and Related Technologies(COBIT). COBIT describes the common requirements that organizations should have in place surrounding their information systems. The COBIT framework is maintained by ISACA. ISO 27001 describes a standard approach for setting up an information security management system, and ISO 27002 goes into more detail on the specifics of information security controls.
2. Performing Vulnerability Assessments (Chapter 15):
   1. NIST provides the community with the Security Content Automation Protocol (SCAP) to meet this need. SCAP provides this common framework for discussion and also facilitates the automation of interactions between different security systems. The components of SCAP most directly related to vulnerability assessment include these:
      1. Common Vulnerabilities and Exposures (CVE) provides a naming system for describing security vulnerabilities
      2. Common Vulnerability Scoring System (CVSS) provides a standardized scoring system for describing the severity of security vulnerabilities
      3. Common Platform Enumeration (CPE) provides a naming system for operating systems, applications, and devices.
      4. Extensible Configuration Checklist Description Format (XCCDF) provides a language for specifying security checklists.
      5. Open Vulnerability and Assessment Language (OVAL) provides a language for describing security testing procedures.
      6. Link: csrc.nist.gov/Projects/Security-Content-Automation-Protocol
   2. Vulnerability Scans: automatically probe systems, applications, and networks, looking for weaknesses that may be exploited by an attacker. The scanning tools used in these tests provide quick, point-and-click tests that perform otherwise tedious tasks without requiring manual intervention. Remember, these tools can be used by attackers as well. There are 4 main categories of vulnerability scans:
      1. Network discovery scans
         1. TCP SYN Scanning
         2. TCP Connect Scanning: Opens a full connetion to the remote system on the specified port. This scan type is used when the user running the scan doesn’t have the necessary permissions to run a half-open scan.
         3. TCP ACK Scanning
         4. UDP Scanning
         5. Xmas Scanning: sends a packet with the FIN, PSH, and URG flags set. A packet with so many flags set is said to be “lit up like a Christmas tree,” leading to the scan’s name.

When nmap scans a system, it identifies the current state of each network port on the system:

- Open: there is an application that is actively accepting connections on that port

- Closed: there’s no application accepting connections on that port

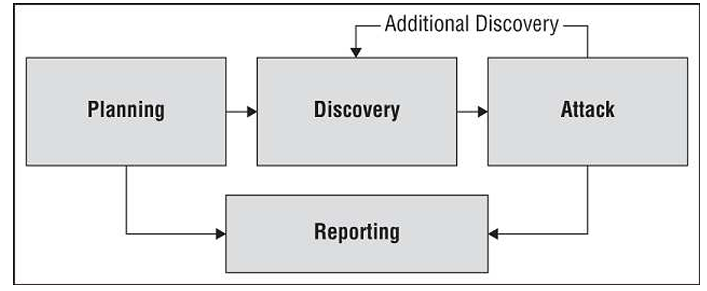
- Filtered: nmap is unable to determine whether a port is open or closed because a firewall is interfering with the connection attempt.

Some jurisdictions consider unauthorized scanning a violation of computer abuse laws and may prosecute individuals for an act as simple as running nmap on a coffee shop wireless network.

The **netstat** command is a useful tool for examining the active ports on a system.

* + 1. Network vulnerability scans: go deeper than discovery scans. They continue on to probe a targeted system or network for the presence of known vulnerabilities. These tools contain databases of thousands of known vulnerabilities, along with tests they can perform to identify whether a system is susceptible to each vulnerability in the system’s database.
       1. False positive report: the scanner falsely reports a vulnerability when there really is no problem
       2. False negative report: far more dangerous is when the vulnerability scanner misses a vulnerability and fails to alert the administrator.
       3. By default, network vulnerability scanners run unauthenticated scans (without having passwords or other special information that would grant the scanner special privileges).
       4. One way to improve the accuracy of the scanning and reduce false positive and false negative reports is to perform **authenticated scans** of systems. In this approach, the scanner has read-only access to the servers being scanned and use that information when analyzing vulnerability testing results.
       5. Learning TCP Ports (important for the CISSP exam):
          1. FTP: 20/21
          2. SSH: 22
          3. Telnet: 23
          4. SMTP: 25
          5. DNS: 53
          6. HTTP: 80
          7. POP3: 110
          8. NTP: 123
          9. Windows File Sharing: 135, 137-139, 445
          10. HTTPS: 443
          11. LPR/LPD: 515
          12. Microsoft SQL Server: 1433/1434
          13. Oracle: 1521
          14. H.323: 1720
          15. PPTP: 1723
          16. RDP: 3389
          17. HP JetDirect printing: 9100
       6. The OWASP maintains a comprehensive list at <https://oiwasp.org/www-community/Vulnerability_Scanning_Tools> The open source OpenVAS scanner also has a growing community of users.
       7. Organizations may also conduct specialized vulnerability assessment of wireless networks. Aircrack-ng is a tool commonly used to perform these assessments by testing the encryption and other security parameters of wireless networks. It can be used in conjunction with passive monitoring techniques that may identify rogue devices on the network.
    2. Web application vulnerability scans: special-purpose tools that scour web applications for known vulnerabilities. When an administrator runs a web application scan, the tool probes the web application using automated techniques that manipulate inputs and other parameters to identify web vulnerabilities. It’s a good practice to run scans in the following circumstances:
       1. Scan all applications when you begin performing web vulnerability scanning for the first time. This will detect issues with legacy applications.
       2. Scan any new application before moving it into a production environment for the first time.
       3. Scan any modified application before the code changes move into production.
       4. Scan all applications on a recurring basis. Limited resources may require scheduling these scans on the priority of the application

In some cases, web application scanning may be required to meet compliance requirements. For example, the PCI DSS requires that organizations either perform web application vulnerability scans at least annually or install dedicated web application firewalls to add additional layers of protection against web vulnerabilities

* + 1. Database vulnerability scans: allow security professionals to scan both databases and web applications for vulnerabilities that may affect database security. **Sqlmap** is a commonly used open source database vulnerability scanner that allows security administrators to probe web applications for database vulnerabilities.
  1. Vulnerability Management Workflow
     1. Detection: the initial identification of a vulnerability normally takes place as the result of a vulnerability scan
     2. Validation: once a scanner detects a vulnerability, administrators should confirm the vulnerability to determine that it is not a false positive report
     3. Remediation: validated vulnerabilities should then be remediated. This may include applying a vendor-supplied security patch, modifying a device configuration, implementing a workaround to avoid the vulnerability, or installing a web application firewall or other control that prevents the exploitation of the vulnerability
  2. Penetration Testing: NIST defines the penetration testing process as consisting of the four phases illustrated:
     1. Planning: includes agreement on the scope of the test and the rules of engagement. It ensures that both the testing team and management are in agreement about the nature of the test and that the test is explicitly authorized.
     2. Information gathering and discovery: uses manual and automated tools to collect information about the target enviroment. This includes performing basic reconnaissance to determine system function (such as visiting websites hosted on the system) and conducting network discovery scans to identify open ports. Testers also use automated tools during this phase to probe for system weaknesses.
     3. Attack: seeks to use manual automated exploit tools to attempt to defeat system security. This step is where penetration testing goes beyond vulnerability scanning.
     4. Reporting: summarizes the results of the penetration testing and makes recommendations for improvements to system security.

Penetration testers commonly use a tool called **Metasploit Framework** to automatically execute exploits against targeted systems. The tests are normally categorized into 3 groups:

- White-Box Penetration Test: provides the attackers with detailed information about the systems they target. This bypasses many of the reconnaissance steps that normally precede attacks.

- Gray-Box Penetration Test: partial knowledge tests. It’s sometimes chosen to balance the advantages and disadvantages of white- and black-box penetration tests. This is particularly common when black-box results are desired but costs or time constraints mean that some knowledge is needed to complete the testing.

- Black-Box Penetration Test: simulates an external attacker trying to gain access to information about the business and technical environment before engaging in an attack.

Breach and Attack Simulations (BAS) platforms: designed to inject threat indicators onto systems and networks in an effort to trigger other security controls. For example, a BAS platform might place a suspicious file on a server, send beaconing packets over a network, or probe systems for known vulnerabilities. The BAS platform is not actually waging attacks, but it’s conducting automated testing of those security controls to identify deficiencies that may indicate the need for control updates or enhancements.

Penetration tests are time-consuming and require specialized resources, but they play an important role in the ongoing operation of a sound information security testing program.

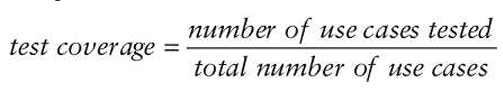
There are many industry-standard penetration testing methodologies that make a good starting point when designing your own program: OWASP Web Security Testing Guide, OSSTMM (Open Source Security Testing Methodology Manual), NIST 800-115, FedRAMP Penetration Test Guidance, or PCI DSS Information Supplement on Penetration Testing as references.

* 1. Compliance Checks: an important part of security testing and assessment programs for regulated firms. It verify that all of the controls listed in a compliance plan are functioning properly and are effectively meeting regulatory requirements. Should perform these checks regularly. Savvy organizations create and maintain compliance plans documenting each of their regulatory obligations and map those to the specific security controls designed to satisfy each objective.

1. Testing Your Software (Chapter 15)
   1. Think about the following characteristics common to many applications in use throughout the modern enterprise:
      1. Software applications often have privileged access to the operating system, hardware, and other resources
      2. Software applications routinely handle sensitive information, including credit card numbers, Social Security numbers, and proprietary business information
      3. Many software applications rely on databases that also contain sensitive information
      4. Software is the heart of the modern enterprise and performs business-critical functions. Software failures can disrupt businesses with very serious consequences
   2. Code Review and Testing
      1. Code review (or peer review): the code review takes many different forms and varies in formality from organization to organization. The most formal code review processes, known as **Fagan inspections**, follow a rigorous review and testing process with six steps: planning, overview, preparation, inspection, rework, and follow-up. The Fagan inspection level of formality is normally found only highly restrictive environments where code flaws may have catastrophic impact. Most organizations use less rigorous processes that include the following:
         1. Developers walking through their code in a meeting with one or more other team members
         2. A senior developer performing manual code review and signing off on all code before moving the code to production
         3. Use of automated review tools to detect common application flaws before moving the code to production
      2. Static application security testing (SAST): evaluates the security of software without running it by analyzing either the source code or the compiled application. Usually, it uses automated tools to detect common software flaws like buffer overflows. In mature development environments, application developers are given access to static analysis tools and use them throughout the design, build, and test process.
      3. Dynamic application security testing (DAST): evaluates the security of software in a runtime environment, often the only option for organizations deploying applications written by someone else. A common example is the use of web application scanning tools (detecting CSRF, SQL injection and so on). It may include the use of **synthetic transactions** (scripted transactions with known expected results) to verify system performance.
         1. Fuzz Testing: a specialized dynamic testing technique that provides many different types of input (either randomly generated or specially crafted to trigger known software vulnerabilities) to software to stress its limits and find previously undetected flaws. It then monitors the performance of the application, watching for software crashes, buffer overflows, or other undesirable and/or unpredictable outcomes.
            1. Mutation (Dumb) Fuzzing: Takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input. It might alter the characters of the content, append strings to the end of the content, or perform other data manipulation techniques. **Zzuf** tool (available as linux command) automates the process of mutation fuzzing by manipulating input according to user specifications.
            2. Generational (Intelligent) Fuzzing: Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program.

Fuzz testing is an important tool, but it has limitations. Fuzz testing should be considered only one tool in a suite of tests performed, and it’s useful to conduct test **coverage analysis** to determine the full scope of the test.

* + 1. Additionally, interactive application security testing (**IAST**) performs real-time analysis of runtime behavior, application performance, HTTP/HTTPS traffic, frameworks, components, and backend connections. Runtime Application Self-Protection (**RASP**) is a tool that runs on a server and intercepts calls to and from an application and validates data requests.
    2. Ethical disclosure: says that security professionals who detect a vulnerability have responsibility to report that vulnerability to the vendor, providing them with an opportunity to develop a patch or other remediation to protect their customers. This disclosure should first be made privately to the vendor, allowing them to correct the problem before it becomes public knowledge. **However**, the ethical disclosure principle also suggests that those reporting a vulnerability should provide the vendor with a reasonable amount of time to correct the vulnerability and, if it’s not corrected, then publicly disclose the vulnerability so that other security professionals may take informed decisions about their future use of the product.
    3. Interface testing: assesses the performance of modules against the interface specifications to ensure that they will work together properly when all the development efforts are complete. There are 3 types of interfaces should be tested during the software testing process:
       1. Application Programming Interfaces
       2. User Interfaces (UIs) including GUIs and command-line interfaces.
       3. Physical Interfaces
    4. Misuse case testing (or abuse case testing): users may try to manipulate input strings to gain access to another user’s account. They might also try to withdraw funds from an account that is already overdrawn. Software testers use abuse case testing to evaluate the vulnerability of their software to these known risks. Testers first enumerate the known misuse cases.
    5. Test Coverage Analysis: helps estimate the degree of testing conducted against the new software. It’s unfortunately impossible to completely test any piece of software.



The test coverage analysis formula may be adapted to use many different criteria. Here are five common criteria:

- Branch coverage: has every if statement been executed under all if and else conditions?

- Condition coverage: has every logical test in the code been executed under all sets of inputs?

- Function coverage: has every function in the code been called and returned results?

- Loop coverage: has every loop in the code been executed under conditions that cause code execute multiple times, only once, and not at all?

- Statement coverage: has every line of code been executed during the test?

* + 1. Website monitoring: Passive monitoring is particularly useful for troubleshooting issues identified by users because it allows the capture of traffic related to that issue. Synthetic monitoring may miss issues experienced by real users if they are not included in the testing scripts, but it’s capable of detecting issues before they actually occur.
       1. Passive monitoring: analyzes actual network traffic sent to a website by capturing it as it travels over the network or reaches the server. Real user monitoring (**RUM**) is a variant of passive monitoring where the monitoring tool reassembles the activity of individual users to track their interaction with a website.
       2. Synthetic monitoring (or active monitoring): performs artificial transactions against a website to assess performance. It may be as simple as requesting a page from the site to determine the response time, or it may execute a complex script designed to identify the results of a transaction.
  1. Implementing Security Management Processes: these processes are a critical feedback loop in the security assessment process because they provide management oversight and have a deterrent effect against the threat of insider attacks. There are several security management reviews:
     1. Log Reviews
        1. SIEM
        2. Windows Group Policy Objects (GPOs): require third-party clients to add syslog support. Administrators use GPOs to deploy logging policies and enforce standard policies throughout the organization.
        3. Logging systems should also make use of the Network Time Protocol (NTP) to ensure that clocks are synchronized on systems sending log entries to the SIEM as well as the SIEM itself.
        4. Information security managers should also periodically conduct log reviews, particularly for sensitive functions, to ensure that privileged users are not abusing their privileges. For example, if an information security team has access to eDiscovery tools that allow searching through the contents of individual user files, security managers should routinely review the logs of actions taken by those administrative users to ensure that their file access relates to legitimate eDiscovery intiatives and does not violate user privacy.
        5. Network flow (NetFlow) logs are particularly useful when investigating security incidents. These logs provide records of the connections between systems and the amount of data transferred.
     2. Account Management: one way to perform account management is to conduct a full review of all accounts. This is typically done only for highly privileged accounts because of the amount of time consumed. The exact process may vary from organization to organization, but here’s one example:
        1. Managers ask system administrators to provide a list of users with privileged access and the privileged access rights. They may monitor the administrator as they retrieve this list to avoid tampering.
        2. Managers ask the privilege approval authority to provide a list of authorized users and the privileges they should be assigned.
        3. The managers then compare the two lists to ensure that only authorized users retain access to the system and that the access of each user does not exceed their authorization.
     3. Disaster Recovery and Business Continuity
        1. Backup verification: part of DLP and BCP. Data protection requirements usually are preventing data loss, data availability, and recovering data after an incident. Consistent backup programs are an extremely important component of these efforts. This may involve reviewing logs, inspecting hash values, or requesting an actual restore of a system or file.
     4. Training and Awareness: many organizations use phishing simulations to evaluate the effectiveness of their security awareness programs.
     5. Key Performance and Risk Indicators: the exact metrics used by security managers for monitoring will vary from organization to organization but may include the following:
        1. Number of open vulnerabilities
        2. Time to resolve vulnerabilities
        3. Vulnerability/defect recurrence
        4. Number of compromised accounts
        5. Number of software flaws detected in preproduction scanning
        6. Repeat audit findings
        7. User attempts to visit known malicious sites

1. Training, Awareness, and Documentation (Chapter 18)
   1. When designing a training plan, consider including the following elements:
      1. Orientation training for all new employees
      2. Initial training for employees taking on a new disaster recover role for the first time
      3. Detailed refresher training for disaster recovery team members
      4. Brief awareness refreshers for all other employees (can be accomplished as part of other meetings and through a medium like email newsletters sent to all employees)
   2. Loose-leaf binders are an excellent way to store disaster recovery plans. You can distribute single-page changes to the plan without destroying an entire forest.
   3. Because of the rapidly changing nature of the disaster recovery and business continuity plans, you might consider publication on a secured portion of your organization’s intranet.
   4. DRP should be treated as an extremely sensitive document and provided to individuals on a compartmentalized, need-to-know basis only.
2. Testing and Maintenance (Chapter 18): For more information on this topic, consult NIST Special Publication 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities Recommendations, available at csrc.nist.gov/publications/detail/sp/800-84/final
   1. The types of tests that you conduct will depend on the types of recovery facilities available to you, the culture of your organization, and the availability of disaster recovery team members.
      1. Read-Through Test: one of the simplest tests to conduct but one of the most critical. You distribute copies of disaster recovery plans to the members of the disaster recovery team for review.
         1. It ensures that key personnel are aware of their responsibilities and have that knowledge refreshed periodically
         2. It provides individuals with an opportunity to review the plans for obsolete information and update any items that require modification because of changes within the organization
         3. In large organizations, it helps identify situations in which key personnel have left the company and nobody bothered to reassign their disaster recovery responsibilities. This is also a good reason why disaster recovery responsibilities should be included in job descriptions.
      2. Structured Walk-Through (or tabletop exercise): members of the disaster recovery team gather in a large conference room and role-pay a disaster scenario.
         1. Usually, the exact scenario is known only to the test moderator, who presents the details to the team at the meeting. The team members then refer to their copies of the disaster recovery plan and discuss the appropriate responses to that particular type of disaster
         2. Some exercises include taking physical actions or at least considering their impact on the exercise. For example, a walk-through might require that everyone leave the building and return home to participate in the exercise (as if the office is inaccessible).
      3. Simulation Test: disaster recovery team members are presented with a scenario and asked to develop an appropriate response. Pretty similar to structured-walk through test but some of these response measures are then tested. This may involve the interruption of noncritical business activities and the use of some operational personnel.
      4. Parallel Test: involve relocating personnel to the alternate recovery site and implementing site activation procedures. The employees relocated to the site perform their disaster recover responsibilities just as they would for an actual disaster. The only difference is that operations at the main facility are not interrupted. The main facilities still run all actual operations and the alternating site is only used for the test.
      5. Full-Interruption Tests: like parallel tests but they involve actually shutting down operations at the primary site and shifting them to the recover site. It’s extremely difficult to arrange, and you often encounter resistance from management.
      6. Lessons Learned: provide everyone involved with the incident response effort an opportunity to reflect on their individual roles in the incident and the team’s response overall.
         1. Most common way to conduct lessons learned is to gather everyone in the same room, or connect them via videoconference or telephone, and ask a trained facilitator (ideally have played no role in the incident response, leaving them to be neutral party who simply helps guide the conversation) to lead a lessons learned session. The facilitator should work with the team leader to document the lessons learned in a report that includes suggested process improvement actions.
         2. Time is important. As time passes, details quickly become fuzzy and memories are lost. The more quickly you conduct a lessons learned session, the more likely it is that you will receive valuable feedback that can help guide future responses.
         3. In SP 800-61, NIST offers a series of questions to use in the lessons learned process:
            1. Exactly what happened and at what times?
            2. How well did staff and management perform in dealing with the incident?
            3. Were documented procedures followed?
            4. Were the procedures adequate?
            5. Were any steps or actions taken that might have inhibited the recovery?
            6. What would the staff and management do differently the next time a similar incident occurs?
            7. How could information sharing with other organizations have been improved?
            8. What corrective actions can prevent similar incidents in the future?
            9. What precursors or indicators should be watched for in the future?
            10. What precursors or indicators should be watched for in the future to detect similar incidents?
            11. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
      7. Maintenance
         1. Minor changes may often be made through through a series of telephone conversations or emails, whereas major changes may require one or more meetings of the full disaster recover team.
         2. A disaster recovery planner should refer to the organization’s business continuity plan as a template for its recovery efforts. This and all the supportive material may need to comply with applicable regulations and reflect current business needs. Business processes such as payroll and order generation should contain specified metrics mapped to related IT systems and infrastructure.
         3. Most organizations apply formal change management processes so that whenever the IT infrastructure changes, all relevant documentation is updated and checked to reflect such changes. Regularly scheduled fire drills and dry runs to ensure that all elements of the DRP are used properly to keep staff trained present a perfect opportunity to integrate changes into regular maintenance and change management procedures. Design, implement, and document changes each time you go through these processes and exercises. Know where everything is, and keep each element of the DRP working properly. In case of emergency, use your recovery plan. Finally, make sure the staff stays trained to keep their skills sharp-for existing support personnel-and use simulated exercises to bring new people up to speed quickly.

Domain 7: Security Operations

1. Apply Foundational Security Operations Concepts (chapter 16)
   1. Need-to-Know and Least Privilege
      1. Need-to-Know Access: Although it’s most often associated with military and government agencies’ clearances, it can also apply in civilian organizations. For example, database administrators may need access to a database server to perform maintenance, but they don’t need access to all the data within the server’s databases. Restricting access based on a need to know helps protect against unauthorized access that could result in a loss of confidentiality
      2. Principle of Least Privilege: in may networks regular users can log on to any computer in the network using a network account. However organizations commonly restrict this privilege by preventing regular users from logging on to servers or restricting users’ access to a single workstation. Additionally, if a user logs on with full administrative privileges and inadvertently installs malware, the malware can assume full administrative privileges of the user’s account.
   2. Separation of Duties (SoD) and Responsibilities: no single person has total control over a critical function or system. It creates a checks-and-balances system. For example, one person approves payment for a valid invoice, but someone else makes the payment. Another way separation of duties is enforced is by dividing the security or administrative capabilities and functions among multiple trusted individuals. **No single person has sufficient access to circumvent or disable security mechanisms.**
   3. Two-Person Control (or two-man rule): requires approvals from 2 individuals for **critical** tasks (like safe deposit boxes in banks often require 2 keys). It ensures peer review and reduces the likelihood of collusion and fraud. Some privilege access management (PAM) solutions create special administrative accounts for emergency use only. The password is split in half so that two people need to enter the password to log on. **Split knowledge** combines the concepts of separation of duties and two-person control into a single solution.
   4. Job rotation (or rotation of duties): employees rotate through jobs or rotate job responsibilities with other employees. It provides peer review, reduces fraud, and enables cross-training making an environment less dependent on any single individual. It can also act as both a deterrent and a detection mechanism.
   5. Mandatory Vacations: can act as both a deterrent and a detection mechanism
   6. Privileged Account Management: in this context, they are administrator accounts or any accounts that have specific elevated privileges.
      1. In Microsoft domains, this includes local administrator accounts (who have full control over a computer), users in the Domain Admins group (who have full control of any computers in a domain), and a users in the Enterprise Admins group (who have full control over all the domains in a forest). Solutions:
         1. It’s based on a just-in-time administration principle. Users are placed in a privileged group and they request permission to use elevated privileges when they need them. The PAM solution approves this request behind the scenes and grants it within seconds by issuing a time-limited ticket (like for 15 minutes, which quickly expires).
         2. On a more basic level, **privileged account management** monitors actions taken by privileged accounts including creating new user accounts, adding new routes to a router table, altering the configuration of a firewall, and accessing system log and audit files.

Reasons that can hange a trusted employee’s behavior can be as simple as a lower-than-expected bonus, a negative performance review, or just a personal grudge against another employee. So, monitoring is important. Additionally, access review audits detect misuse of these privileges.

* + 1. In Linux, this include anyone using the root account or granted root access via sudo.
    2. TA17-239A (released by DHS and FBI): helps detect advanced persistent threat (APT) activities:
       1. Accessing and deleting logs
       2. Creating and manipulating accounts (such as adding new accounts to the Administrators group)
       3. Controlling communication paths (such a opening port 3389 to enable the Remote Desktop Protocol and/or disabling the host firewall)
       4. Running various scripts (including PowerShell, batch, and JavaScript files)
       5. Creating and scheduling tasks (such as one that logged their accounts out after 8 hours to mimic the behavior of a regular user)
  1. Service Level Agreenment (SLAs): stipulates performance expectations and often includes penalties if the vendor doesn’t meet these expectations. Additionally, organizations sometimes use a memorandum of understanding (MOU) documenting the intention of two entities to work together toward a common goal. It’s less formal and doesn’t include any monetary penalties if one of the parties doesn’t meet its responsibilities.

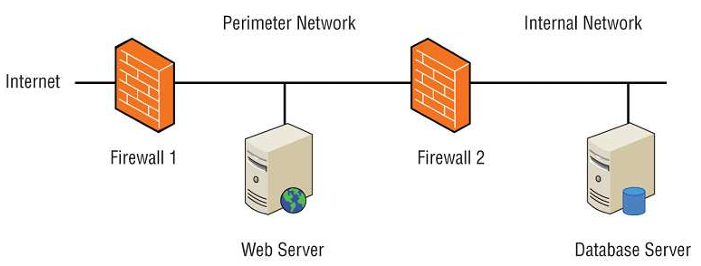
1. Address Personnel Safety and Security (chapter 16)
   1. Duress system: useful when personnel are working alone. If a group of people break into the building, the guard probably can’t stop them on their own. Owever, a guard can raise an alarm with a duress system. Security systems often include **code words or phrases** that personnel use to verify false alarm. In case if criminals apprehended the guard, the guard could skip the phrase and instead make up a story. The monitoring entity would recognize that the guard skipped the code phrase and send help.
   2. Travel: includes simple things such as verifying a person’s identity before opening the hotel door. If room service is delivering complimentary food, a call to the front desk can verify if this is valid or part of a scam. Employees should be warned about risks associated with electronic devices when traveling:
      1. Sensitive Data: employees should worry
      2. Malware and Monitoring Devices: employees should worry
      3. Free Wi-Fi: employees should worry
      4. VPNs: employees should have this
   3. Emergency Management plans and practices: help an organization address personnel safety and security after a disaster.
   4. Security Training and Awareness: when addressing personnel safety and security, training programs should stress the iportance of protecting people. Military warships travel into war zones during times of conflict, putting personnel at risk. However, they also do endless training to protect lives. Organizations rarely face the same level of risk but should still prioritize the value of human lives.
2. Apply Resource Protection: Imaging, change management, and patch management topics are discussed later in this chapter. Information is stored on media, so an essential part of resource protection is protecting media. This includes when storing media and when the media reaches the end of its lifecycle.
   1. Media Management: steps taken to protect media and data stored on media. Media includes tapes, optical media such as CDs, and DVDs, portable USB drives, internal hard drives, solid-state drives, USB flash drives, backups (often contained on tapes), any type of hard-copy data, and maybe many portable devices like smartphones.
   2. Media Protection Techniques:
      1. Sensitive information should be stored in a secure location with strict access controls. Additionally, any location used to store media should have temperature and humidity controls to prevent losses due to corruption.
      2. Some technical controls to restrict devices access from computer systems like blocking the use of USB drives and/or detect and record when users attempt to use them. In some situations, a written security policy prohibits the use of USB flash drives, and automated detection methods detect and report any violations. Some organizations sell IronKey flash drives that include multiple levels of built-in protection with several authentication mechanisms and, maybe, built-in AES 256-bit hardware-based encryption. Active antimalware software on the flash drie helps preent malware from infcting the drive. Some products include additional management solutions, allowing administrators to manage the devices remotely. Administrator can reset passwords, activate auditing, and update the devices from a central location.
      3. Some other ideas fit for certain devices:
         1. Tape Media: As a best practice, organizations should keep at least two copies of backups (one for immediate usage if necessary and one kept at a secure location off site). Some useful guidelines for managing tape media:
            1. Keep new media in its original sealed packaging until It’s needed to protect it from dust and dirt.
            2. When opening a media package, take extra caution not to damage the mdia in any way. This includes avoiding sharp objects and not twisting or flexing the media.
            3. Avoid exposing the media to temperature extremes; it shouldn’t be stored close to heaters, radiators, air conditioners, or other sources of extreme temperatures.
            4. Do not use media that has been damaged, exposed to abnormal levels of dust and dirt, or dropped
            5. Media should be transported from one site to another in a temerature-controlled vehicle
            6. Media should be protected from exposure to the outside environment; avoid sunlight, moisture, humidity, heat, and cold. It should be acclimated for 24 hours before use.
            7. Appropriate security should be maintained over media from the point of departure to the secured offsite storage facility. Media is vulnerable to damage and theft at any point during transportation
            8. Appropriate security should be maintained over media throughout the lifetime of the media based on the classification level of data on the media.
            9. Consider encrypting backups to prevent unauthorized disclosure of data if the backup tapes are lost or stolen.
         2. Mobile Devices (including smartphones and tablets): Chapter 9, “Security Vulnerabilities, Threats, and Countermeasures,” covers mobile devices in much more depth.
         3. Managing Media Lifecycle: Reusable media is subject to a mean time to failure (MTTF) that is sometimes represented in the number of times it can be reused or the number of years you can expect to keep it. However, many variables affect the lifetime of media and can reduce these estimates. It’s important to **monitor backups** for errors and use them as a guide to gauge the lifetime in your environment. Chapter 10, “Physical Security Requirements,” covers MTTF in more depth.

Note: MTTF is different from mean time between failures (MTBF). MTTF is normally calculated for items that will not be repaired when they fail, such as a tape. In contrast, MTBF refers to the amount of time expected to elapse between failures of an item that personnel will repair, such as a computer server.

1. Managed Services in the Cloud
   1. Shared Responsibility with Cloud Service Models (already covered above)
   2. Scalability and Elasticity
      1. Scalability: refers to the ability of a system to handle additional workloads by adding additional resources. Imagine a server has 16 GB of RAM, but it can support 64GB of RAM. It’s possible to shut down the server and add additional RAM to scale it up.
      2. Elasticity refers to a system’s ability to add and remove resources dynamically, based on increasing or decreasing load. Imagine an e-commerce server with 16 GB of RAM and a four-core processor. Marketing launches an excellent advertising campaign along with a sale. Suddenly, the server is overwhelmed with traffic. A cloud provider that supports elasticity can dynamically add more RAM and processors to meet the increased workload. When the sale ends and the workload decreases, the cloud provider can dynamically remove the additional resources.
      3. Chapter 9 covers virtualization concepts. Virtualization technologies commonly support elasticity, too.
2. Perform Configuration Management (CM) (e.g., provisioning, baselining, automation for systems): helps ensure that systems are deployed in a secure, consistent state throughout their lifetime.
   1. Provisioning new systems: refers to installing and configuring the operating system and needed applications.
      1. Disable all unused services. As an example, a file server needs services that allow users to access files, but file servers rarely use FTP. If the server is not using FTP, it should be disabled.
      2. Close all unused logical ports. These are often closed by disasbling unused services.
      3. Remove all unused applications. Some applications automatically add additional applications. If these aren’t used, they should be removed.
      4. Change default passwords.
   2. Baselining: a starting point. An operating system baseline identifies all the settings to harden specific systems.
   3. Using Images for Baselining: It’s an overall three-step process:
      1. An administrator starts by installing the operating system and all desired applications on a computer (labeled as the baseline system in the figure). The administrator then configures the system with relevant security and other settings to meet the organization’s needs. Personnel then perform extensive testing to ensure that the system operates as expected before proceeding to the next step.
      2. Next, the administrator captures an image of the system using **imaging software** and stores it on a server (labeled as an Image Server in the figure). It’s also possible to store images on external hard drives, USB drives, or DVDs.
      3. Personnel then deploy the image to systems as needed. These systems often require additional configuration to finalize them, such as giving them unique names. However, the overall configuration of these systems is the same as the baseline system. In a worst-case scenario, malware can be injected into an image and then deployed to systems within the network.
   4. Automation: It’s common to combine imaging with other automated methods for baselines. Microsoft’s operating systems include Group Policy. Administrators can configure a Group Policy setting one time and automatically have the setting apply to all the computers in the domain.
      1. It’s becoming common to make registry changes for some Windows systems. Attackers are using PowerShell in offensive attacks quite often. By modifying some registry settings, administrators limit these attacks’ effectiveness and detect them when they start.
3. Managing Change: helps reduce unanticipated outages caused by unauthorized changes
   1. An administrator can change one system to resolve a problem but unknowingly cause a problem in other systems. The web server is accessible from the internet and accesses the database on the internal network. Administrators have configured appropriate ports on Firewall 1 to allow internet traffic to the web server and appropriate ports on Firewall 2 to allow the web server to access the database server. The administrator may see an unrecognized open port on Firewall 2 and decide to close it in the interest of security. After a bunch of hooting, hollering, blamestorming, and finger-pointing, someone realizes that a needed port on Firewall 2 is closed. They open the port and resolve the problem until the administrator closes it again or starts tinkering with Firewall 1.

Frustrated administrators may decide to add a group of users to an Administrators group within the network. Users will now have all the access they need, improving their ability to use the network, and they will no longer bother the administrators with access requests. However, granting administrator access in this way directly violates the least privilege principle and significantly weakens security.

Many of the configuration and change management concepts in use today are derived from ITIL (formally an acronym for Information Technology Infrastructure Library) published by the UK. The ITIL Core includes 5 publications addressing the overall lifecycle of systems. ITIL focuses on best practices that an organization can adopt to increase overall availability.



* 1. Change Management: a mandatory element for some security assurance requirements (SARs) in the **ISO Common Criteria**. Common tasks within a change management process are as follows:
     1. Request the change: The website automatically logs the request in a database, which allows personnel to track the changes. It also allows anyone to see the status of a change request.
     2. Review the change: In some cases, the change may require approval at a formal change review board or change advisory board (CAB) after extensive testing.
     3. Approve/reject the change: They also record the response in the change management documentation. In some cases, the change review board might require the creation of a rollback or backout plan, ensuring the system can be returned to its original condition.
     4. Test the change
     5. Schedule and implement the change: it can be implemented with the least impact on the system
     6. Document the change: helps all interested parties aware of it
  2. Versioning: version control used in software configuration management. It helps keep track of changes over time to deployed software
  3. Configuration Documentation: identifies the current configuration of systems, identifies who is responsible for the system and its purpose and lists all changes applied to the baseline. It’s more common to store this information in files or databases today, but it can be inaccessible during an outage.

1. Managing Patches and Reducing Vulnerabilities
   1. Systems to Manage:
      1. Doesn’t only apply to workstations and servers. It’s any computing device with an operating system.
      2. Embedded systems (or IoT-Internet of Things) are any devices that have a CPU like camera systems, smart televisions, household appliances, automobiles, medical devices, and more.
      3. Mentioned many times, mobile devices can be managed with MDM softwares that deploy patches.
   2. Patch Management: common steps within an effective patch management program:
      1. Evaluate patches: see if it’s applicable
      2. Test patches: the worst-case scenario is that a system will no longer start after applying a patch
      3. Approve the patches: it’s common to use a change management process as part of the approval process
      4. Deploy the patches
      5. Verify that patches are deployed: Many deployment tools include the ability to audit systems. Many vulnerability assessment tools include the ability to check systems to ensure that they have appropriate patches.
   3. Vulnerability management: regularly identifying vulnerabilities, evaluating them, and taking steps to mitigate risks associated with them. In many cases, one person or group would be responsible for keeping systems patched, and another person or group would be responsible for verifying that the systems are patched.
   4. Vulnerability Scans: the reports may recommend applying patches or making specific configuration or security setting changes
   5. Common Vulnerabilities and Exposures: you can view the CVE database maintained by MITRE (cve.mitre.org)
2. Conducting Incident Management (Chapter 17: Preventing and Responding to Incidents): primary goal of incident management is to minimize the impact on the organization.
   1. Defining an Incident:
      1. An incident: any event that has a negative effect on the confidentiality, integrity, or availability of an organization’s assets.
      2. A computer security incident: result of an attack or the result of malicious or intentional actions on the part of the users.
         1. RFC 2350 (Expectations for Computer Security Incident Response) defines both a security incident and a computer security incident as “any adverse event which compromises some aspect of computer or network security.”
         2. NIST SP 800-61, Computer Security Incident Handling Guide, defines a computer security incident as “a violation or imminent threat of vilation of computer security policies, acceptable use policies, or standard security practices.”
         3. Organizations commonly define the meaning of a computer security incident within their security policy or incident management plans. The definition is usually one or two sentences long and includes examples of common events that the organization classifies as security incidents, such as the following:
            1. Any attempted network intrusion
            2. Any attempted DoS attack
            3. Any detection of malicious software
            4. Any unauthorized access of data
            5. Any violation of security policies
   2. Incident Management Steps



* + 1. Detections: common methods used to detect potential incidents and how these methods report the incidents:
       1. Intrusion detection and prevention systems (described later in this chapter) send alerts to administrators when they detect a potential incident. Many IT professionals are classified as first responders for incidents. They are similar to medical first responders, who have outstanding skills and abilities to provide medical assistance at accident scenes. The medical first responders have specific training to help them determine the difference between minor and major injuries
       2. Antimalware software will often display a pop-up window to indicate when it detects malware.
       3. Many automated tools regularly scan audit logs looking for predefined events, such as the use of special privileges. When they detect specific events, they typically send an alert to administrators
       4. End users sometimes detect irregular activity and contact technicians or administrators for help. When users report events, such as the inability to access a network resource or update a system, it alerts IT personnel about a potential incident.
    2. Response: organizations have a designated incident response team-sometimes called a computer incident response team (CIRT) or computer security incident response team (CSIRT) activated during a major security incident but doesn’t typically activate the team for minor incidents. After an investigation is over, management may decide to prosecute responsible individuals. It’s important to protect all data as evidence during the investigation (Chapter 19, “Investigations and Ethics”). If any possibility of prosecution exists, team members take extra steps to protect the evidence. This ensures that the evidence can be used in legal procedures.
    3. Mitigation: In some cases, responders take steps to mitigate the incident, but without letting the attacker know that the attack has been detected. This allows security personnel to monitor the attacker’s activities and determine the scope of the attack. Organizations sometimes choose not involve law enforcement to avoid negative publicity or an intrusive investigation. However, this is not an option if personal information is exposed.
    4. Reporting: a major incident may reuqire completely rebuilding a system. If an organization has effective configuration management and change management programs, these programs will provide the necessary documentation to ensure the rebuilt systems are configured properly. Things to double-check include the following:
       1. ACLs, which include firewall or router rules
       2. Services and protocols, ensuring that unneeded services and protocols are disabled or removed
       3. Patches, ensuring that all up-to-date patches are installed
       4. User accounts, ensuring that they have changed from their default configurations
       5. Compromises, ensuring that any known compromises have been reversed

In some cases, an attacker may have installed malicious code on a system during an attack. The most secure method of restoring a system after an incident is completely rebuilding the system from scratch.

* + 1. Remediation: this step includes performing a root cause analysis

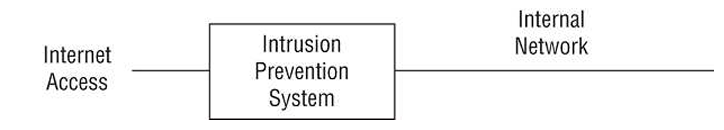
Root cause analysis: examines the incident to determine what allowed it to happen. After identifying a vulnerability that can be mitigated, this stage will recommend a change.

* + 1. Lessons Learned: Remember, the output of this stage can be fed back to the detection stage of incident management. It’s common for the incident response team to create a report when they complete a lessons learned review. Management will decide what recommendations to implement and is responsible for the remaining risk for any recommendations they reject.
  1. Delegating Incident Management to Users: Close to each computer was a checklist that identified common symptoms of malware infection. The checklist instructed them to disable or disconnect the network adapter and contact the help desk to report the issue. By disabling or disconnecting the network adapter, they helped contain the malware to their system and stopped it from spreading.

1. Implementing Detective and Preventive Measures:
   1. Chapter 2, “Personnel Security and Risk Management Concepts,” discusses controls in more depth
      1. Preventive Control: attempts to thwart or stop unwanted or unauthorized activity from occurring (like fences, locks, biometrics, separation of duties policies, job rotation policies, data classification, access control methods, encryption, smart cards, callback procedures, security policies, security awareness training, antivirus software, firewalls, and IPSs.
      2. Detective Control: attempts to discover or detect like security guards, motion detectors, recording and reviewing of events captured by security cameras or closed-circuit television (CCTV), job rotation policies, mandatory vacation policies, audit trails, honeypots or honeynets, IDSs, violation reports, supervision and reviews of users, and incident investigations.
   2. Basic Preventive Measures: many of these steps are described in more depth in other areas of the book but are listed here as an introduction to this section:
      1. Keep systems and application up to date
      2. Remove or disable unneeded services and protocols
      3. Use intrusion detection and prevention systems
      4. Use up-to-date antimalware software
      5. Use firewalls
      6. Implement configuration and system management processes
   3. Understanding Attacks: this section provides an overview of many common attacks. Chapter 7 covers some cryptographic attacks; Chapter 12 covers different types of network-based attacks; Chapter 14 covers various access control attacks; and Chapter 21 covers various attacks related to malicious code and applications.
      1. Botnets (or bots/zombies): bot herder is typically a criminal who controls all the computers in the botnet via one or more command-and-control (C&C or C2) servers. Bot herders usually send DDoS attacks, send spam and phishing emails, or rent the botnets out to other criminals. The malware sometimes installs **keyloggers** to capture user keystrokes and send them back to the attacker. Many malware infections are browser based, allowing user systems to become infected when the user is surfing the web. Most browsers support **sandboxing** (covered later in this chapter) to isolate web applications, but some browsers include the ability to disable sandboxing.
      2. DoS attacks and DDoS attack
      3. SYN Flood Attack: a common DoS attack
      4. Smurf and Fraggle Attacks: both are DoS attacks. Smurf attack floods the victim with ICMP echo packets. It a spoofed broadcast ping request using the IP address of the victim as the source IP address. However, RFC 2644 (released in 1999) changed the standard default for routers so that they do not forward directed broadcast traffic. When administrators correctly configure routers in compliance with RFC 2644, a network cannot be an amplifying network, limiting smurf attacks to a single network. It’s also common to disable ICMP on firewalls, routers, and even many servers to prevent this type of attack using ICMP. Fraggle attacks (similar to smurf attack) use UDP packets over UDP ports 7 and 19. A variant of a fraggle attack is a UDP flooding attack using random UDP ports.
      5. Ping Flood:
         1. Ping of Death: use oversized ping packets.
         2. Teardrop: fragments data packets, making them difficult or impossible to be put back together by the receiving system, often causing the systems to crash.
         3. Land: sends spoofed SYN packets using the victim’s IP address as **both** the source and **destination** IP address. A variant is a banana attack, which redirects outgoing messages from a system back to the system, shutting down all external communication.
      6. Usually, buffer overflow errors can be prevented with patches. Additionally, production systems should not include untested code or allow the user of system or root-level privileges from applications.
      7. Zero-Day Exploit: Here are some examples:
         1. Attacker discovers a vulnerability first
         2. Vendor learns of vulnerability but hasn’t released a patch
         3. Vendor releases patch and systems are attacked within 24 hours: organizations often take time to evaluate and test a patch before applying it. Microsoft typically releases patches on the second Tuesday of every month, commonly called “Patch Tuesday.” Attackers often try to reverse-engineer the patches to understand them and then exploit them the next day, commonly called “Exploit Wednesday.” Additionally, honeypots give administrators an opportunity to observe attacks and may reveal an attack using a zero-day exploit.
      8. Man-in-the-Middle Attacks (MiTM): Some MiTM attacks are thwarted by keeping systems up to date with patches. An intrusion detection system cannot usually detect MiTM or hijack attacks, but it can detect abnormal activities. Many users often use VPNs to avoid these attacks. Some VPNs are hosted by an employee’s organization, but there are also several commercially available VPNs that anyone can use, typically at a cost.
      9. Sabotage: a criminal act of destruction or disruption committed against an organization by an employee.
   4. Intrusion Detection and Prevention Systems: IDSs are an effective method of detecting many DoS and DDoS attacks. An IPS includes all the capabilities of an IDS but can also take additional steps to stop or prevent intrusions. If desired, administrators can disable an IPS’s extra features, essentially causing it to function as an IDS. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems, provides comprehensive coverage of both intrusion detection and intrusion prevention systems, but for brevity uses IDPS throughout the document to refer to both.
      1. Knowledge- and Behavior-Based Detection for IDS
         1. Knowledge-Based Detection (signature-based detection or pattern-matching detection): uses signatures similar to the signature definitions used by antimalware software. The antimalware application has a database of known malware and checks files against the database looking for a match. Just as antimalware software must be regularly updated with new signatures from the antimalware vendor, IDS databases must be regularly updated with new attack signatures. IDS vendors commonly provide automated methods to update the signatures.
         2. Behavior-Based Detection: doesn’t use signatures but instead compares activity against a baseline of normal performance to detect abnormal behavior. Once it has accumulated enough baseline data (often created over a finite period such as a week) to determine normal activity, it can detect abnormal activity that may indicate a malicious intrusion or event. If the network is modified, the baseline needs to be updated. Some products continue to monitor the network to learn more about normal activity and will update the baseline on the observations. Chapter 21 covers user and entity behavior analytics (UEBA) functions. UEBA tools create user profiles (similar to a baseline for a network) based on individual behavior. They then watch for deviations in normal behavior that may indicate malicious activity.

It can be labeled an **expert system** or a **pseudo-artificial intelligence system** because it can act like a human expert by evaluating current events against known events. Its significant benefit is that it can detect newer attacks that have no signatures and are not detectable with the signature-based method

* + 1. IDS Response
       1. Passive Response: Many 24-hour network operations centers (NOCs) have central monitoring screens viewable by everyone in the main support center. For example, a single wall can have multiple large-screen monitors providing data on different elements of the NOC. The IDS alerts can be displayed on one of these screens to ensure that personnel are aware of the event.
       2. Active Response: can modify the environment using several different methods. For example, if an IDS detects a SYN flood attack from a single IP address, the IDS can change the ACL to block all traffic from this IP address.
    2. Host- and Network-Based IDSs
       1. HIDS:
          1. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs can’t detect like infections where an intruder has infiltrated a system and is controlling it remotely.
          2. Although many vendors recommend installing host-based IDSs on all systems, this isn’t common due to cost and usability. HIDSs are more costly to manage than NIDSs because they require administrative attention on each system, whereas NIDSs usually support centralized administration.
          3. Additionally, it will often consume a significant amount of system, degrading the host system’s performance.
          4. HIDSs are easier for an intruder to discover and disable, and their logs are maintained on the system, making the logs susceptible to modification during a successful attack.
       2. NIDS:
          1. Can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console like SIEM system. These sensors can monitor traffic at routers, firewalls, network switches that support port mirroring, and other types of network taps.
          2. Some organizations implement the use of TLS decryptors that detects TLS traffic, takes steps to decrypt it, and sends the decrypted traffic to an IDPS for inspection. A TLS decryptor is often a standalone hardware appliance dedicated to this function, but it can be within an IDPS solution, a next-generation firewall, or some other appliance.
          3. However, Advanced persistent threats (APTs) often encrypt traffic before exfiltrating it out of a network. The encryption is typically performed on a host before establishing a connection with a remote system and sending it.
          4. Switches are often used as a preventive measure against rogue sniffers.
          5. The NIDS central console is often installed on a hardened single-purpose computer, making it operate almost invisibly.
          6. An NIDS has very little negative effect on the overall network performance. When it’s deployed on a single-purpose system, it doesn’t adversely affect any other computer’s performance.
          7. Adding additional systems to balance the load is possible
          8. NIDS can often discoer the source of an attack by performing Reverse Address Resolution Protocol (RARP) or reverse DNS lookups. It’s also possible to discover te source of spoofed IPs with some investigation.
          9. It won’t know if an attack affected specific systems, user accounts, files, or applications.
    3. Intrusion Prevention Systems (IPS)
       1. A distinguishing difference between an NIDS and a network-based IPS (NIPS) is that the NIPS is placed inline with the traffic. This allows the NIPS to prevent an attack from reaching a target. The active NIDS can take steps to block an attack after it starts but can’t prevent it.



* + - 1. An NIPS can use knowledge-based detection and/or behavior-based detection (like any other IDS). Additionally, it can log activity and provide notification to administrators just as an IDS would.
      2. A current trend is the replacement of NIDSs with NIPSs.
    1. Specific Preventive Measures
       1. Honeypots and Honeynets: an organization can legally use a honeypot as an **enticement** device if the intruder discovers it through no outward efforts of the honeypot owner. Enticed attackers make their own decisions to perform illegal or unauthorized actions. **Entrapment**, which is illegal, occurs when the honeypot owner actively solicits visitors to access the site and then charges them with unauthorized intrusion. It’s entrapment when you trick or encourage someone into performing an illegal or unauthorized action.
       2. Warning Banners: inform users and intruders about basic security policy guidelines. These typically remind authorized users of the content in acceptable use agreements.
       3. Antimalware: Organizations often use a central server to deploy antimalware software, download updated definitions, and push these definitions out to the clients.
       4. Whitelisting and Blacklisting (allow list and deny list): It’s important to understand that a system would only use one list, either an allow list or a deny list.
          1. Some allow lists identify applications using a hashing algorithm. The Apple iOS running on iPhones and iPads is an example of an extreme version of an allow list. Although it’s possible for users to bypass security and jailbreak their iOS devices, most users don’t do so, partly because it voids the warranty.
          2. Using a deny list is a good option if administators know which applications they wanna block.
       5. Firewalls: basic guidelines can provide a lot of protection against attacks:
          1. Block directed broadcasts on routers
          2. Block private IP addresses at the border
          3. Firewalls include rules within an ACL to allow specific traffic and end with an implicit deny rule.
          4. Ping uses ICMP, so it’s common to block pings by blocking ICMP echo requests at border firewalls. This prevents the pings from reaching the internal network from the Internet. The Internet Assigned Numbers Authority (IANA) maintains a list of well-known ports matched to protocols.
          5. Second-generation firewalls add additionally filtering capabilities. An application-level gateway firewall filters traffic based on specific application requirements and circuit-level gateway firewalls filter traffic based on the communications circuit. Third-generation firewalls (stateful inspection firewalls and dynamic packet filtering firewalls) filter traffic based on its state within a stream of traffic.
          6. Application firewalls control traffic going to or from a specific application or service. For example, web application firewall (WAF) can block SQL injection attacks and XSS attacks. This can be processor intensive, so the WAF filters traffic going to the web server but not all network traffic.
          7. A next-generation firewall (NGFW) functions as a unified threat management (UTM) device. NGFW can identify and block malicious traffic. It can filter malware using definition files and/or whitelists and blacklists. It also includes intrusion detection and/or intrusion prevention capabilities.
       6. Sandboxing: many antimalware vendors use virtualization as a sandboxing technique to observe the behavior of malware.
       7. Third-party security services: some organizations often outsource some of the services, and PCI DSS requires organizations to ensure that service providers also comply with PCI DSS requirements. PCI DSS doesn’t allow organizations to outsource their responsibilities.
    2. Logging and Monitoring
       1. Logging Techniques: Logs are often referred to as audit logs, and logging is often called audit logging. However, auditing is more than just logging.
          1. Common Log Types:

Security Logs: record access to resources such as files. Many systems automatically record access to key system files but require an administrator to enable auditing on other resources before logging access.

System Logs: record system events such as when a system starts or stops, when services start or stop, or when service attributes are modified. Attackers sometimes modify the attributes of logs. For example, a service might be set to Disabled, but the attacker can change it to Manual, allowing the attacker to start it at will. Logs that detect when systems reboot, or when services stop or are modified, can help administrators discover potentially malicious activity.

Application Logs: record information for specific applications. Application developers choose what to record in the application logs.

Firewall Logs: can record events related to any traffic that reaches a firewall. It often doesn’t log the packet’s actual contents.

Proxy Logs: include the ability to record details such as what sites specific users visit and how much time they spend on these sites.

Change Logs: useful to track approved changes and helpful as part of DRP (like returning a system to its last known state after a disaster).

* + - * 1. Protecting Log Data:

It’s common to store copies of logs on a central system (like SIEM systems) to protect it.

Organizations often have strict policies mandating backups of log files including retention times. Some government regulations require organizations to keep archived logs indefinitely.

Don’t keep unnecessary logs. If regulations require an organization to keep logs for one year but the organization has 10 years of logs, a court order can force personnel to retrieve relevant data from these 10 years of logs.

The Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) specifies the following as the minimum security requirements for audit data:

Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity

Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

* + - 1. The Role of Monitoring:
         1. Audit Trails: records created when information about events and occurrences is stored in one or more databases or log files. They provide a record of system activity and can reconstruct activity leading up to and during security events.

It’s a passive form of detective security control, serving as a deterrent in the same manner that closed-circuit television (CCTV) or security guards do. However, more and more advanced attackers take the time to locate and delete logs that might have recorded their activity. This has become a standard practice with many APTs.

They provide a before-and-after picture of the state of resources, systems, and assets. Because data in audit trails can be so valuable, it’s important to ensure that the logs are protected to prevent modification or deletion.

Monitoring and Accountability:

It’s possible to promote positive user behavior and compliance with the organization’s security policy by monitoring activity.

Legislation often requires specific monitoring and accountability practices (like Sarbanes-Oxley Act of 2002), the HIPPA, and EU privacy laws that many organizations must abide by.

Accountability is necessary at every level of business, from the frontline infantry to the high-level commanders overseeing daily operations.

Monitoring and Investigations: One important consideration is ensuring that logs have accurate timestamps and that these timestamps remain consistent throughout the environment (setting up an internal NTP server). NIST operates several time servers that support authentication. Once an NTP server is properly configured, the NIST servers will respond with encrypted an authenticated time messages.

Monitoring and Problem Identification: They can record system failures, OS bugs, and software errors in addition to malicious attacks. Some log files can even capture the contents of memory when an application or system crashes.

* + - * 1. Monitoring Techniques

Log analysis: a detailed and systematic form of monitoring in which the logged information is analyzed for trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. It isn’t necessarily in response to an incident but instead a periodic task.

When manually analyzing logs, administrators simply open the log files and look for relevant data. Searching 10 different archived logs for a specific event or ID code can take some time, even when using built-in search tools.

Multiple vendors sell operations management software that actively monitors systems’ security, health, and performance throughout a network.

SIEM/SEM/SIM: a centralized application to automate the monitoring of systems on a network. They include agents installed on remote systems that monitor for specific events known as alarm triggers. When the trigger occurs, the agents report the event back to the central monitoring software. It often sophisticated correlation engines. These engines are a software component that collects the data and aggregates it looking for common attributes. It then uses advanced analytic tools to detect abnormalities and sends alerts to security administrators.

Syslog: RFC 5424 (the Syslog Protocol) describes the syslog protocol??? which is used to send event notification messages. A centralized syslog server receives these syslog messages from devices on a network.

Sampling (or data extraction): extract specific elements from a large collection of data to construct a meaningful representation.

Clipping Levels: Clipping is a form of nonstatistical sampling. It selects only events that exceed a clipping level. Instead of raising an alarm for every single failed logon attempt, a clipping level can be set to raise an alarm only if it detects five failed logon attempts within a 30-minute period.

Other Monitoring Tools:

Keystroke monitoring: recording the keystrokes a user performs on a physical keyboard (used with keyloggered)

Traffic Analysis and Trend Analysis (sometimes called **network flow monitoring**): forms of monitoring that examine the flow of packets rather than actual packet contents.

* + - * 1. Log Management: all the methods used to collect, process, and protect log entries.

After a system forwards log entries to a SIEM system, it’s acceptable to delete the log entries. Systems doesn’t usually delete logs from the original system right away. **Rollover logging** allows administrators to set a maximum log size. When the log reaches that size, the system begins overwriting the oldest events in the log.

Another option is to create and schedule a PowerShell script to regularly archive the files and copy them to another location (like a backup server using a UNC path).

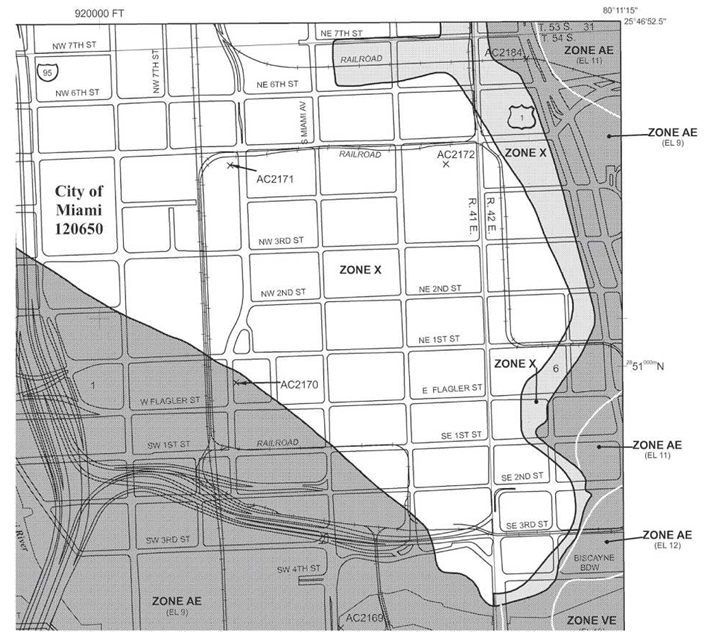
* + - * 1. Egress Monitoring: monitor traffic leaving a network to the Internet.

Some common methods used to detect or prevent data exfiltration are DLP techniques and monitoring for steganography:

Possible to detect steganography attempts if you have both the original file and a file you suspect with hash algorithm.

Advanced implementation of watermarking is digital watermarking. However, advanced attackers (like APTs sponsored by nation-states, commonly encrypt data before sending it out of the network).

1. The Nature of Disaster (Chapter 18)
   1. Natural Disasters:
      1. Earthquakes: The U.S. Geological Survey considers the following states to have the highest earthquake hazard risk: Alaska, Arkansas, California, Hawaii, Idaho, Illinois, Kentucky, Missouri, Montana, Nevada, Oregon, South Carolina, Tennessee, Utah, Washington, and Wyoming.
      2. Floods: flooding results from the gradual accumulation of rainwater in rivers, lake, sand other bodies of water than then overflow their banks and flood the community.
         1. Flash floods strike when a sudden severe storm dumps more rainwater on an area than the ground can absorb in a short period of time. Floods can also occur when dams are breached.
         2. Large waves caused by seismic activity, or tsunamis, combine the awesome power and weight of water with flooding (during the 2011 tsunami in Japan). This tsunami amply demonstrated the enormous destructive capabilities of water and the havoc it can wreak on various businesses and economies when it triggered an unprecedented nuclear disaster at Fukushima.
         3. According to government statistics, flooding is responsible for approximately $8 billion in damage to businesses and homes each year in the US. In the US, most general business policies do not cover flood damage, and you should investigate obtaining specilized government-backed flood insurance under the Federal Emergency Management Agency’s (FEMA) National Flood Insurance Program. FEMA’s National Flood Insurance Program is responsible for completing a flood risk assessment for the entire US and providing this data to citizens in graphical form.
         4. You’ll find that they often combine several different types of confusing terminology. First, the shading indicates the likelihood of a flood occuring in an area. Areas shaded with the darkest color are described as failing within the 100-year floodplain. This means that the government estimates the chance of flooding in that area are 1 in 100. Those shaded more lightly lie within the 500-year floodplain, meaning that there is a 1 in 500 annual risk of flood.



* + 1. Storms: Hurricanes and tornadoes can turn everyday objects such as trees, lawn furniture, and even vehicles into deadly missiles. Hailstorms bring a rapid onslaught of destructive ice chunks falling from the sky and risk of lightning. For this reason, your BCP should detail appropriate mechanisms to protect against lightning-induced damage, and your DRP should include adequate provisions for power outages and equipment damage that might result from a lightning strike. DR specialists in hurricane-prone areas should periodically check the website of the National Weather Services’s National Hurricane Center (nhc.noaa.gov) during hurricane season.
    2. Fires: Some regions of the world are susceptible to wildfires during the warm season. These fires, once started, spread in somewhat predictable patterns, and fire experts working with meteorologists can produce relatively accurate forecasts of a wildfire’s potential path.
    3. Pandemics
    4. Other Natural Events: many parts of the world are subject to volcanic eruptions. Other localized natural occurrences include monsoons in Asia, tsunamis in the South Pacific, avalanches in mountainous regions, and mudslides in the western US. Make use of local resources such as government emergency preparedness teams, civil defense organizations, and insurance claim offices to help guide your efforts.
  1. Human-Made Disasters:
     1. Fires: may result from carelessness, faulty electrical wiring, improper fire protection practices, arson, or other reasons.
     2. Acts of Terrorism: The Insurance Information Institute issued a study one year after the attacks that estimated the total damage from the attacks in New York City at $40 billion. Policy riders and endorsements are sometimes available, but often at extremely high cost. If your BCP or DRP includes insurance as a means of financial recovery (as it probably should!), you should check your policies and contact your insurance professionals to ensure that you’re still covered.
     3. Bombings/Explosions: the effects of bombings and explosions are like those caused by a large-scale fire. However, it’s more difficult to prevent and it relies on the physical security measures.
     4. Power Outages: Critical business systems are often protected by uninterruptible power supply (UPS) devices. Check your UPSs regularly as they are often overlooked until they become necessary. Some UPSs contain self-testing mechanisms that report problems automatically. Be sure to audit the number and type of devices plugged into each UPS. An adequate backup generator could make a huge difference when the survival of your business is at stake.
        1. Does your BCP include provisions to keep your business viable during a prolonged period without power?
        2. What’s your planning horizon?
        3. Do you need enough fuel and other supplies to last for 48 hours?
        4. Does your DRP make ample preparations for the timely restoration of power even if the commercial power grid remains unavailable?
     5. Network, Utility, and Infrastructure Failures:
        1. Do any of your critical business systems rely on water, sewers, natural gas, or other utilities? Also consider regional infrastructure such as highways, airports, and railroads. If a major storm knocks out the water supply to your facilities and you need to keep those facilities up and running, can you supply your employees with enough drinking water to meet their needs? Enough water for fire protection systems? Fire often cause serious damage in areas ravaged by storms, earthquakes, and other disasters that might also interrupt the delivery of water.
        2. You must also think about your internet connectivity as a utility service. Do you have sufficient redundancy in your connectivity options to survive or recover quickly from a disaster? If you have redundant providers, do they have any single points of failure? For example, do they both enter your building in a single fiber conduit that could be severed? If there are no alternative fiber ingress points, can you supplement a fiber connection with wireless connectivity? Do your alternate processing sites have sufficient network capacity to carry the full burden of operations in the event of disaster?
     6. Hardware/Software Failures: BCP/DRP teams must provide adequate redundancy in their systems. Because of financial constraints, it isn’t always feasible to maintain fully redundant systems. Instead, they should plan how replacement parts can be quickly obtained and installed. After all, how many organizations could do without telephones for three days while a critical private branch exchange (PBX) component is en route from an overseas location to be installed on site?
     7. Strikes/Picketing: If a large number of your employees walk out at the same time, what impact would that have on your business? How long would you be able to sustain operations without the regular full-time employees that staff a certain area? Labor issues normally fall outside the purview of cybersecurity teams, offering a great example of an issue that should be included in a disaster recover plan but requires input and leadership from other business functions, such as human resources and operations.
     8. Theft/Vandalism: such as scrappers stealing copper in wires, air-conditioning systems, plumbing, and power subsystems or vandals destroying sensors, can negatively impact critical business functions. Insurance provides some financial protection against these events (subject to deductibles and limitations of coverage), but acts of this kind can cause serious damage to your business, on both a short-term and a long-term basis.
        1. Offsite Challenges to Security: Aaron knows the threats to confidential data firsthand, working as a security officer for a prominent and highly visible computing enterprise. Bethany is one of his more troublesome employees because she’s constantly taking her notebook computer off site without properly securing its contents. Bethany must come to understand and appreciate the importance of keeping sensitive information secure. If may suffice to point out to Bethany that the employee handbook clearly states that employees whose behavior leads to the unauthorized disclosure or loss of information assets are subject to loss of pay or termination.
        2. It’s a good idea to keep extra inventory of items with a high pilferage rate, such as RAM chips and mobile devices. It’s also a good idea to keep such materials in secure storage and to require employees to sign such items out whenever they are used.

1. Understand System Resilience, High Availability, and Fault Tolerance
   1. A single point of failure (SPOF): any component that can cause an entire system to fail.
   2. System resilience: ability of a system to maintain an acceptable level of service during an adverse event. In some contexts, it refers to the ability of a system to return to a previous state after an adverse event. System resilience implies that the cluster can fail back to the original server after the original server is repaired.
   3. Fault tolerance: the ability of a system to suffer a fault but continue to operate. It’s achieved by adding redundant components, such as additional disks within a properly configured RAID array or additional servers within a failover clustered configuration.
   4. High availability: the use of redundant technology components to allow system to quickly recover from a failure after experiencing a brief disruption. It’s often achieved through the use of load balancing and failover servers.
   5. Technology professionals measure the objective and effectiveness of these controls by the percentage of the time that a system is available.
   6. Protecting Hard Drives: A RAID array includes 2 or more disks and most RAID configurations will continue to operate even after one of the disks fails. Some common RAID configurations are as follows:
      * 1. RAID-0 (or stripping): uses 2 or more disks and improves the disk subsystem performance, but it does not provide fault tolerance.
        2. RAID-1 (or mirroring): uses 2 disks that hold the same data. Depending on the hardware used and which drive fails, the system may be able to continue to operate without intervention, or the system may need to be manually configured to use the drive that didn’t fail.
        3. RAID-5 (or stripping with parity): uses 3 or more disks with the equivalent of one disk holding parity information. This parity information allows the reconstruction of data through mathematical calculations if a single disk is lost. If any single disk fails, the RAID array will continue to operate, though it will be slower.
        4. RAID-6 (an alternative approach to disk striping with parity): functions like RAID-5 but stores parity information on two disks, protecting against the failure of two separate disks but requiring a minimum of four disks to implement.
        5. RAID-10 (known as RAID 1 + 0 or stripe of mirrors): it’s configured as two or more mirrors (RAID-1), with each mirror configured in a striped (RAID-0) configuration. It uses at least 4 disks but can support more as long as an even number of disks are added. It will continue to operate even if multiple disks fail, as long as at least one drive in each mirror continues to function. For example, if it had three mirrored sets (called M1, M2, and M3 for this example) it would have a total of 6 disks. If one drive in M1, one in M2, and one in M3 all failed, the array would continue to operate. However, if two drives in any of the mirrors failed, such as both dries in M1, the entire array would fail.

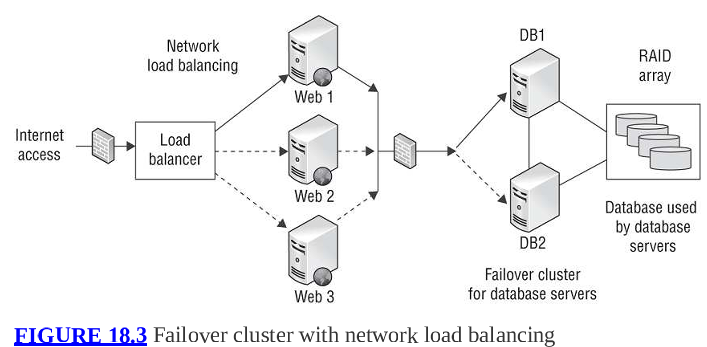
Fault tolerance is not the same as a backup. Occasionally, management may balk at the cost of backup tapes and point to the RAID array, saying that the data is already backed up. However, if a catastrophic hardware failure destroys a RAID array, all the data is lost unless a backup exists. Similarly, if an accidental deletion or corruption destroys data, it cannot be restored if a backup doesn’t exist.

Both software- and hardware-based RAID solutions are available.

- Software-based systems require the operating system to manage the disks in the array and can reduce overall system performance. They are inexpensive as the don’t require additional hardware other than the additional disk(s).

- A hardware RAID can increase availability of critical component. Hardware-based RAID arrays typically include spare drives that can be logically added to the array. If one disk fails, the hardware senses the failure and logically swaps out the faulty drive with a good spare. Additionally, most hardware-based arrays support **hot swapping**, allowing technicians to replace failed disks without powering down the system. A **cold-swappable** RAID requires the system to be powered down to replace a faulty drive.

* 1. Protecting Servers:
     1. Failover cluster: include 2 or more servers, and if one of the servers fails, another server in the cluster can take over its load in an automatic process called **failover**.



You can see that both DB1 and DB2 have access to the data in the database. This data is stored on a RAID array, providing fault tolerance for the disks. The load balancer can be hardware or software based, and it balanced the client load across the 3 servers. If any of these servers fail, the load balancer can sense the failure and stop sending traffic to that server.

Many IaaS providers offer load-balancing services that automatically scale resources on an as-needed basis. These services also incorporate health checking that can automatically restart servers that are not functioning properly. When designing cloud environments, be sure to consider the availability of data centers in different regions of the world. If you’re already load balancing multiple servers, you may be able to place those servers in different geographic regions and availability zones within those regions to add resiliency in addition to scalability.

Some systems provide automatic fault tolerance for servers. In a Microsoft domain with two or more domain controllers, each domain controller will regularly replicate Active Directory data with the others so that all the domain controllers have the same data. If one fails, computers within the domain can still find the other domain controller(s) and the network can continue to operate. Electronic vaulting, remote journaling, and remote mirroring are discussed later in this chapter.

* 1. Protecting Power Sources: The goal of a UPS is to provide power long enough to complete a logical shutdown of a system, or until a generator is powered on and providing stable power.
     1. Generators provide power to systems during long-term power outages. Generators also require a steady fuel supply-they commonly use diesel fuel, natural gas, or propane. In addition to making sure that you have sufficient fuel on hand, you should take steps to ensure that you can be delivered fuel on a regular basis in the event of an extended emergency. If you have contracts in place with suppliers, you’re much more likely to receive fuel in a timely manner.
  2. Trusted Recovery: provides assurances that after a failure or crash, the system is just as secure as it was before the failure or crash occurred. It may be automated or require manual intervention by an administrator depends on the failure. Systems can be designed so that they fail in a fail-secure state or a fail-open state. Two elements of the recover process:
     1. Failure preparation: includes system resilience and fault-tolerant methods in addition to a reliable backup solution.
     2. System recovery: forced to reboot into a single-user, nonprivileged state.
        1. The system should reboot so that a normal user account ca be used to log in and so that the system does not grant unauthorized access to users.
        2. It also includes the restoration of all affected files and services actively in use on the system at the time of the failure or crash. Any missing or damaged files are restored, any changes to classification labels are corrected, and settings on all security critical files are then verified.

The Common Criteria (CC) include a section on trusted recovery that is relevant to system resilience and fault tolerance. It defines four types of trusted recovery:

* + 1. Manual Recovery: administrators manually perform the actions necessary to implement a secured or trusted recovery after a failure or system crash.
    2. Automated Recovery: the system is able to perform trusted recovery activities to restore itself against at least one type of failure.
    3. Automated Recovery without Undue Loss: similar to automated recovery. However, it includes mechanisms to ensure that specific objects are protected to prevent their loss. The method would include steps to restore data or other objects. It may include additional protection mechanisms to restore corrupted files, rebuild data from transaction logs, and verify the integrity of key system and security components.
    4. Function Recovery: systems that support function recovery are able to automatically recover specific functions. This state ensures that the system is able to successfully complete the recovery for the functions, or that the system will be able to roll back the changes to return to a secure state.
  1. Quality of Service (QoS) controls: protect the availability of data networks under load and protect the quality of the end-user experience. Some of the factors contributing to QoS are as follows:
     1. Bandwidth
     2. Latency: the time it takes a packet to travel from source to destination
     3. Jitter: variation in latency between different packets
     4. Packet Loss: require retransmission when packets are lost
     5. Interference: Electrical noise, faulty equipment, and other factors may corrupt the contents of packets.

A QoS device might be programmed to prioritize a videoconference traffic from the executive conference room over video streaming from an intern’s computer. QoS may also include specific security requirements, such as requiring encryption for certain types of traffic.

1. Recovery Strategy
   * 1. Transaction logs — files that record every small change or transaction made since the last backup.
   1. Business Unit and Functional Priorities: most organizations will complete a BIA (helps identify and prioritize critical business functions as well so that you can define which functions you want to restore after a disaster or failure and in what order) in BCP. A BIA also identifies costs related to failures that include loss of cash flow, equipment replacement, salaries paid to clear work backlogs, profit losses, opportunity costs from the inability to attract new business, and so forth. Such failures are assessed in terms of potential impacts on finances, personnel, safety, legal compliance, contract fulfillment, and quality assurance, preferably in monetary terms to make impacts comparable and to set budgetary expectations. A detailed list, broken down into specific business processes listed in order of priority (process-oriented list), would be a much useful deliverable, which is reflective of real-world conditions. The final result should be a checklist of items in priority order, each with its own risk and cost assessment, and a corresponding set of recovery objectives and milestones (including MTTR, MTD, RTO, and RPO).
   2. Crisis Management
      1. The individuals in your business who are most likely to first notice an emergency situation should be fully trained in disaster recovery procedures and know the proper notification procedures and immediate response mechanisms.
      2. Many things that normally seem like common sense may slip in the minds of panicked employees seeking to flee an emergency. Continuous training on disaster recovery responsibilities is necessary.
      3. It’s a science and an art form. If your training budget permits, investing in crisis training for your key employees is a good idea. At least some of your employees know how to handle emergency situations properly and can provide all-important “on-the-scene” leadership to panic-stricken coworkers.
   3. Emergency Communications: Employees participating in disaster recovery efforts should be instructed to refer media inquiries to the public relations team. Sometimes, all normal means of communications are damaged.
      1. A disaster of any significance is easily noticed, but if an organization is unable to keep the outside world informed of its recovery status, the public is apt to fear the worst and assume that the organization is unable to recover.
      2. The organization should be able to communicate internally during a disaster so that employees know what’s expected of them (like if they are return to work or report to another location).
   4. Workgroup Recovery: restore workgroups to the point that they can resume their activities in their usual work locations. If you have several subsidiary organizations that are in different locations and that perform tasks similar to the tasks that workgroups at your office perform, you may want to consider temporarily relocating those workgroups to the other facility and having them communicate electronically and via telephone with other business units until they’re ready to return to the main operations facility. However, large organizations may have difficulty finding recovery facilities capable of handling the entire business operation. In this case, independent recover of different workgroup is appropriate (so that teams don’t wait for each other to get back to work).
   5. Alternate Processing Sites
      1. Cold Sites: standby facilities large enough to handle the processing load of an organization and equipped with appropriate electrical and environmental support systems
         1. No computing facilities (hardware or software) preinstalled and no active broadband communications links
         2. Many cold sites have at least a few copper telephone lines, and some may have standby links that can be activated with minimal notification.
         3. A well-depicted cold site setup is in the film Boiler Room.
      2. Hot Sites:
         1. Backup facility is maintained in constant working order, with a full complement of servers, workstations, and communications links ready to assume primary operations responsibilities. The servers and workstations are all preconfigured and loaded with appropriate operating system and application software.
         2. The data on the primary site servers is periodically or continuously replicated to corresponding servers at the hot site, ensuring that the hot site has up-to-date data.
         3. Depending on the bandwidth available between the sites, hot site data may be replicated instantaneously. If that’s the case, operators could move operations to the hot site at a moment’s notice. If it’s not the case, disaster recovery mangers have options to activate the hot site:
            1. If there’s sufficient time before the primary site must be shut down, they can force replication between the two sites right before the transition of operational control.
            2. If replication is impossible, managers may carry backup tapes of the transaction logs form the primary site to the hot site and manually reapply any transactions that took place since the last replication.
            3. If there are no available backups and it isn’t possible to force replication, the disaster recovery team may simply accept the loss of some portion of the data. This should only be done when the loss is within the organization’s RPO.

The cost is extremely high (essentially doubles an organization’s budget for hardware, software, and services and requires the use of additional employees to maintain the site). It might opt to use a shared hot site facility managed by an outside contractor. However, the inherent danger in these facilities is that they may be overtaxed in the event of a widespread disaster and be unable to service all clients simultaneously. Investigate these issues thoroughly, both before

* + 1. Warm Sites: Unlike hot sites, warm sites don’t typically contain copies of the client’s data.
       1. The main requirement in bringing a warm site to full operational status is the transportation of appropriate backup media to the site and restoration of critical data on the standby servers.
       2. Activation of a warm site typically takes at least 12 hours from the time a disaster is declared. Switchover times for most hot sites are often measured in seconds or minutes, and complete cutovers seldom take more than an hour or two.
       3. Warm sites avoid significant telecommunications and personnel costs inherent in maintaining a near-real-time copy of the operational data environment.
       4. Like hot sites and cold sites, warm sites may also be obtained on a shared facility basis. Be sure to have a “no lockout” policy (don’t lock out something after a certain conditions are met) written into your contract guaranteeing you the use of an appropriate facility even during a period of high demand. It’s a good idea to physically inspect the facilities and the contractor’s operational plan to reassure yourself that the facility will indeed be able to back up the “no lockout” guarantee should push ever some to shove.
    2. Mobile Sites: non-mainstream alternatives to traditional recovery sites.
       1. Include all the environmental control systems necessary to maintain a safe computing environment.
       2. Larger corporations sometimes maintain these sites on a “fly-away” basis, ready to deploy them to any operating location around the world via air, rail, sea, or surface transportation. Smaller firms might contract with a mobile site vendor in their local area to provide these services on an as-needed basis.
       3. Mobile sites are usually configured as cold sites or warm sites, depending on the disaster recovery plan they are designed to support. It’s unusual to configure a mobile site as hot site because you seldom know in advance where a mobile site will need to be deployed.

Consider hardware replacement supplies when determining mobile sites and recovery sites in general:

- Employ “in-house” (means you own it already, not that it’s necessarily housed under the same roof as your production) replacement, whereby you store extra and duplicate equipment at a different but nearby location.

- SLA-type agreement with a vendor to provide quick response and delivery time in the event of a disaster. However, even a 4-, 12-, 24-, or 48-hour replacement hardware contract from a vendor doesn’t provide a reliable guarantee that delivery will actually occur. There are too many uncontrollable variables to rely on this second option as your sole means of recovery.

* + 1. Cloud Computing: Companies wishing to maintain their own datacenters may choose to use these IaaS options as backup service providers. Storing ready-to-run images with cloud providers is often quite cost effective and allows the organization to avoid incurring most of the operating cost until the cloud site activates in a disaster. For organizations that already operate their technology resources in the cloud (they don’t get a free pass on disaster recovery), they must think about how they will handle issues that arise within their cloud environment then design and configure their use of cloud services to take advantage of redundancy options, geographic dispersion, and similar considerations.
    2. Mutual Assistance Agreements (MAAs, also called reciprocal agreements): rarely implemented in real-world practice. Under an MAA, two organizations pledge to assist each other in the event of a disaster by sharing computing facilities or other technological resources. They appear to be extremely cost effective at first glance-it’s not necessary for either organization to maintain expensive alternate processing sites (described in previous sections). Many MAAs are structured to provide one of the levels of service described. In the case of a cold site, each organization may simply maintain some open space in their processing facilities for the other organization to use in the event of a disaster. In the case of a hot site, the organizations may host fully redundant servers for each other. Drawbacks are these:
       1. The parties might trust each other to provide support in the event of disaster. However, when push comes to shove, the nonvictim might renege on the agreement. A victim may have legal remedies available, but this doesn’t help the immediate disaster recovery effort.
       2. Cooperating organizations should be located close enough to facilitate transportation of employees between sites but not too close that may suffer at the same time.
       3. Confidentiality concerns (like the handling of healthcare or financial data) or business concerns (like trade secrets or other intellectual property issues).
  1. Database Recovery: selecting solutions that lose data beyond your RPO pose unwarranted risk, whereas selecting those that are more aggressive than your RPO may incur unnecessary costs. You’ll need to analyze your organization’s computing requirements and available resources to select the option best suited to your firm and within the boundaries of your RPO.
     1. Electronic Vaulting: Database backups are moved to a remote site using bulk transfer.
        1. Remember that there may be a significant delay between the time you declare a disaster and the time your database is ready for operation with current data. If you decide to activate a recovery site, technicians will need to retrieve the appropriate backups from the electronic vault and apply them to the soon-to-be production servers at the recovery site.
        2. Be careful when considering vendors for an electronic vaulting contract (since definitions vary widely in the industry). Insist on a written definition of the service that will be provided, including the storage capacity, bandwidth of the communications link to the electronic vault, and the time necessary to retrieve vaulted data in the event of disaster.
        3. Periodically test your electronic vaulting setup like giving disaster recovery personnel a “surprise test,” asking them to restore data from a certain day.
        4. Electronic vaulting introduces the potential for significant data loss. In the event of a disaster, you
     2. Remote Journaling:
        1. Data transfer still occur in a bulk transfer mode, but they occur on a more frequent basis, usually once every hour and sometimes more frequently.
        2. Unlike electronic vaulting (where entire database backup files are transferred), remote journaling setups transfer copies of the database transaction logs containing the transactions that occurred since the previous bulk transfer.
        3. Example: Imagine a company backs up their entire database every night at 2 a.m. (this is a "bulk backup"). Now imagine their server crashes at 4 p.m. the next day. If they only had the 2 a.m. backup, they'd lose all data from 2 a.m. to 4 p.m. But, if they also have transaction logs sent every few minutes to a remote site, they can:
           1. Restore the 2 a.m. backup (“bulk backup”, also a electronic vaulting process)
           2. Replay every transaction log in order from 2 a.m. to 4 p.m (now it’s remote journaling process)
           3. Recover the system with minimal or zero data loss.
        4. Remote journaling is similar to electronic vaulting in that transaction logs transferred to the remote site are not applied to a live database server but are maintained in a backup device.
     3. Remote Mirroring: most advanced database backup solution (and the most expensive one).
        1. A live database is maintained at the backup site.
        2. The remote server receives copies of the database modifications (transaction logs) at the same time they are applied to the production server at the primary site. Hence, almost no or very low RTO.
        3. It’s a popular database backup strategy for organizations seeking to implement a hot site. Be sure to take into account the infrastructure and personnel costs required to support the mirrored server, as well as the processing overhead that will be added to each database transaction on the mirrored server.

1. Recovery Plan Development: Don’t expect to sit down and write the full plan in one sitting. It’s likely that the DRP team will go through many draft documents before reaching a final written document that satisfies the operational needs of critical business units and falls within the resource, time, and expense constraints of the disaster recovery budget and available personnel.
   * 1. Executive summary providing a high-level overview of the plan
     2. Department-specific plans
     3. Technical guides for IT personnel responsible for implementing and maintaining critical backup systems
     4. Checklists for individual on the disaster recovery team
     5. Full copies of the plan for critical disaster recovery team members
     6. Managers and public personnel will have a simple document that walks them through a high-level view of the coordinated symphony that is an active disaster recovery effort without requiring interpretation from team members busy with tasks directly related to that effort.
     7. Visit the Professional Practices library at drii.org/resources/professionalpractices/EN. Others worth considered are BCI Good Practice Guidelines (GPG), ISO 27001, and NIST SP 800-34, Contigency Planning Guide for Federal Information Systems.
   1. Emergency Response plans: They are often put together in the form of checklists provided to responders. Always sort this checklist in priority order. The plan should include clear criteria for activation of the DRP, define who has the authority to declare a disaster, and then discuss notification procedures (discussed later).
   2. Personnel and Communications: a list of personnel to contact in the event of a disaster includes key members of the DRP team as well as personnel who execute critical disaster recovery tasks throughout the organization. It also should include alternate means of contact (pager numbers, mobile phone numbers, and so on) as well as backup contacts for each role should the primary contact be incommunicado or unable to reach the recovery site for one reason or another. Be sure to consult with the individuals in your organization responsible for privacy before assembling and disseminating a telephone notification checklist.
   3. Assessment: When the disaster recovery team arrives on site, one of their first tasks is to assess the situation. If you’re unable to survive minor amounts of data loss, your ability to tolerate faults is low.
   4. Backups and Off-site Storage:
      1. Full Backups: Store a complete copy of the data contained on the protected device. Once a full backup is complete, the archive bit on every file is reset, turned off, or set to 0.
      2. Incremental Backups: Store only those files that have been modified since the time of the most recent full or incremental backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated.
      3. Differential Backups: Store all files that have been modified since the time of the most recent full backup. Only files that have the archive bit turned on, enabled, or set to 1 are duplicated.
      4. A common **strategy** is to perform full backups over the weekend and incremental or differential backups on a nightly basis. The specific method of backup (and procedures) determined based on the RPO values.
      5. The toughest obstacle to a solid backup strategy is human nature, so a simple, transparent, and comprehensive strategy is the most practical.
      6. Disk-to-Disk Backup (D2D) solutions: used by many enterprises for some portion of their disaster recovery strategy. Note that organizations seeking to adopt an entirely D2D approach must remember to maintain geographical diversity. Many organizations solve this problem by hiring managed service providers to manage remote backup locations.
      7. Backup Best Practices:
         1. Backups should be scheduled during the low peak periods.
         2. Build sufficient capacity to handle a reasonable amount of growth over a reasonable amount of time into your backup solution.
         3. Murphy’s law dictates that a server never crashes immediately after a successful backup. To avoid the problem with periods, you may deploy some form of real-time continuous backup, such as RAID, clustering, or server mirroring.
         4. Only include necessary information in backups. If your RTO dictates a rapid recovery capability, the storage cost of maintaining many copies of the operating system may be justified by the fact that it makes restoring the entire system from a stored image quite fast.
         5. Remember to test your organization’s recovery processes. Organizations often rely on the fact that their backup software reports a successful backup and fail to attempt recovery until it’s too late to detect a problem.
      8. Tape Rotation Strategies: can be implemented manually using a pencil and a calendar or automatically by using either commercial backup software or a fully automated hierarchical storage management (HSM) system (an automated robotic backup jukebox consisting of 32 or 64 optical or tape backup devices). All the drive elements within an HSM system are configured as a single drive array (a bit like RAID).
         1. The Grandfather-Father-Son (GFS) strategy
         2. The Tower of Hanoi strategy
         3. The Six Cartridge Weekly Backup strategy
   5. Software Escrow Arrangements: To protect themselves, the company makes an agreement where the source code for the software is stored (or "escrowed") by a trusted third party if something happens to the developer.
      1. This third party then maintains updated backup copies of the source code in a secure fashion.
      2. The agreement between the end user and the developer specifies “trigger events,” such as the failure of the developer to meet terms of a SLA or the liquidation of the developer’s firm.
   6. Utilities: several utilities provide critical elements of your infrastructure-electric power, water, natural gas, sewer service, and so on. The DRP should contain procedures (or information) to troubleshoot these services.
   7. Logistics and Supplies: DRP team is responsible for providing food, water, shelter, and appropriate facilities.
   8. Recovery vs. Restoration:
      1. **Recovery** involves bringing business operations and processes back to a working state (supposed to be within the MTD/RTO or else the company fails).
      2. **Restoration** involves bringing a business facility and environment back to a workable state (salvage team members’ job).
      3. If the original location no longer exists, a new primary spot is selected. The salvage team must rebuild or repair the IT infrastructure. Fortunately, the salvage team has more time to work than the recovery team. The salvage team can ensure the reliability of the new IT infrastructure by returning the least mission-critical processes to the restored original site to stress-test the rebuilt network. Then, more important processes are transferred. Your DRP should specify the criteria used to determine when it’s appropriate to return to the primary site and guide the DRP recovery and salvage teams through an orderly transition.
2. Training, Awareness, and Documentation (already covered above).
3. Investigations: Failure to abide by the correct procedures may violate the civil rights of those individual(s) being investigated and could result in a failed prosecution or even legal action against the investigator.
   1. Investigation Types:
      1. Administrative Investigations: examine either operational issues (related to the organization’s computing infrastructure) or a violation of the organization’s policies. Administrative investigations may quickly transition to another type of investigation.
         1. Administrators conducting an operational investigation will only conduct analysis necessary to reach their operational conclusions. No need thorough or well documented as resolving the issue is the primary goal.
         2. Root cause analysis: seeks to identify the reason that an operational issue occurred
         3. Administrative investigations that are not operational in nature may require a stronger standard of evidence as they may result in sanctions against an individual. No appropriate standard of evidence in these investigations. Security professionals should consult with the sponsor of the investigation and legal team to determine appropriate evidence collection, handling, and retention guidelines.
      2. Criminal Investigations: Most criminal cases must meet the beyond a **reasonable doubt** standard of evidence. Criminal investigations must follow strict evidence collection and preservation processes.
      3. Civil Investigations: usually use the weaker **preponderance of the evidence** standard (simply requiring that the evidence demonstrate that the outcome of the case is more likely than not).
      4. Regulatory Investigations: maybe conducted by government agencies (with a standard of proof) when believe that an individual or corporation has violated administrative law.
      5. Industry Standards: some regulatory investigations may not involve government agencies (like PCI DSS). These standards are not laws but are contractual obligations entered into by the participating organizations. Failure to participate in these investigations (or negative investigation results) may lead to fines or other sanctions.
      6. Electronic Discovery (eDiscovery) process: facilitates the processing of electronic information for disclosure (like a digital investigation). The Electronic Discovery Reference Model (EDRM, for more information, see edrm.net/resources/frameworks-and-standards/edrm-model) describes a standard process for conducting eDiscovery with nine aspects:
         1. Information Government: Ensures that information is well organized for future eDiscovery efforts.
         2. Identification: Locates the information that may be responsive to a discovery request when the organization believes that litigation is likely.
         3. Preservation: Ensures that potentially discoverable information is protected against alteration or deletion.
         4. Collection: Gathers the relevant information centrally for use in the eDiscovery process.
         5. Processing: Screens the collected information to perform a “rough cut” of irrelevant information, reducing the amount of information requiring detailed screening.
         6. Review: Examines the remaining information to determine what information is relevant to the request and removing any information protected by attorney-client privilege.
         7. Analysis: Performs deeper inspection of the content and context of remaining information.
         8. Production: Places the information into a format that may be shared with others and delivers it to other parties, such as opposing counsel.
         9. Presentation: Displays the information to witnesses, the court, and other parties.
      7. Evidence: artifacts (maybe maintained and used in court) like computers, mobile devices, and network devices, the logs and data generated by those devices, and many other forms of evidence. NIST SP 800-86 is a great reference: [www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response](http://www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response)
         1. Admissible Evidence: must meet all 3 of these requirements (determined by a judge, prior to being discussed in open court):
            1. The evidence must be relevant to determining a fact.
            2. The fact that the evidence seeks to determine must be material (that is, related) to the case.
            3. The evidence must be competent, meaning it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it’s not competent.
            4. Types of Evidence:

Real Evidence (object evidence): things that may actually be brought into a court of law. Depending on the circumstances, real evidence may also be **conclusive evidence** like DNS that is incontrovertible.

Documentary Evidence: any written items (can be computer logs) brought into court to prove a fact at hand. Must be authenticated. Must comply these rules:

The best evidence rule: the original document must be introduced (copies won’t be accepted unless certain exceptions to the rule apply).

The parol evidence rule: when an agreement between parties is put into written form, the written document is assumed to contain all the terms of the agreement and no verbal agreements may modify the written agreement.

Chain of Evidence: When evidence is labeled to preserve the chain of custody, the label should include the following types of information about the collection:

General description of the evidence

Time and date the evidence was collected

Exact location the evidence was collected from

Name of the person collecting the evidence

Relevant circumstances surrounding the collection

Testimonial Evidence: either verbal testimony in court or written testimony in a recorded deposition. Witnesses must take an oath agreeing to tell the truth, and they must have personal knowledge on which their testimony is based.

Hearsay Rule: when a witness offers testimony in court, they must normally avoid the act of hearsay, meaning that they cannot testify about what someone else told them outside of court because the court has no way to substantiate that evidence and find it admissible.

Demonstrative Evidence: used to support testimonial evidence or help a witness explain a concept or clarify an issue.

* + - * 1. Artifacts, Evidence Collection, and Forensic Procedures: When analyzing digital evidence, it’s best to work with a copy of the actual evidence whenever possible.

Media Analysis: involves with magnetic media (like hard disks, tapes…) or optical media (CDs, DVDs, Blu-ray discs…).

When gathering information from storage devices, analysts should never access hard drives or other media from a live system. Instead, they should power off the system (after collecting other evidence), remove the storage device, and then attach the storage device to a dedicated forensic workstation, using a **write blocker** (hardware adapters that physically sever the portion of the cable used to connect the storage device that would write data to the device, reducing the likelihood of accidental tampering with the device).

After that, the analyst should immediately calculate a cryptographic hash of the device contents and then use forensic tools to create a forensic image of the device: a bitwise copy of the data stored on the device

The analyst should then compute the cryptographic hash of that image to ensure that it’s identical to the original media contents.

The original image file should be preserved as evidence. The copies of that image (verifying the integrity of the hash) is used for analysis.

In-Memory Analysis: When gathering the contents of memory, analysts should use trusted tools to generate a **memory dump** file and place it on a forensically prepared device (like USB drive). As with other types of digital evidence, that analyst should verify the authenticity (using hash algorithm) of the dump file, preserve the original collected dump, and work from copies of that dump file.

Network Analysis: often difficult to reconstruct due to the volatility of network (generally not preserved). It often depends on either prior knowledge that an incident is under way or the use of preexisting security controls that log network activity:

Intrusion detection and prevention system logs

Network flow data captured by a flow monitoring system

Packet captures deliberately collected during an incident

Logs from firewalls and other network security devices

SPAN port on a switch or network tap are useful for capturing packets. Analysts then compute cryptographic hashes of the original evidence files and work only with copies.

Software Analysis: When malicious insiders are suspected, the analyst may be asked to conduct a review of software code, looking for backdoors, logic bombs, log files from application or database servers, privilege escalations, or other security vulnerabilities and application attacks (covered in chapter 21, “Malicious Code and Application Attacks.” The National Software Reference Library (NSRL) maintained by the NIST includes the cryptographic hash values for over 130 million known applications, making it easier for forensic analysts to detect authentication and manipulated files (www.nist.gov/itl/ssd/software-quality-group/national-software-reference-library-nsrl).

Hardware/Embedded Device Analysis

Personal computers

Smartphones

Tablet computers

Embedded Computers in cars, security systems, and other devices

The International Organization on Computer Evidence (IOCE) outlines six principles to guide digital evidence technicians as they perform media analysis, network analysis, and software analysis in the pursuit of forensically recovered evidence:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.

- Upon seizing digital evidence, actions taken should not change that evidence.

- When it’s necessary for a person to access original digital evidence, that person should be trained for this purpose.

- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.

- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.

- Any agency that’s responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

* + - * 1. Investigation Process.

Gathering Evidence: an important consideration is whether the employee has a reasonable expectation of privacy.

The person who owns the evidence could voluntarily surrender it or grant consent to a search. In most cases, asking for evidence from a suspected attacker just alerts the suspect that you are close to taking legal action

You could get a court to issue a subpoena (court order)

Plain view doctrine (a legal exception of 4th amendment): as the name suggested, if the evidence is in plain view, the officer can seize it.

Search warrant: a court order authorize the officer to search a specific location

Exigent circumstances: urgent situations allowing the officer to make a warrantless entry

Calling in Law Enforcement: complicated decision that should involve senior management officials

Conducting the Investigation

Never conduct your investigation on an actual system that was compromised. Take the system offline, make a backup, and use the backup to investigate the incident.

Never attempt to “hack back”

If in doubt, call in expert assistance. If you don’t wanna call in law enforcement, contact a private investigations firm with specific experience in the field of computer security investigations

Interviewing Individuals and interrogation: should be performed only by trained investigators. Improper techniques may jeopardize the ability of law enforcement to successfully prosecute an offender. Always consult an attorney.

Data Integrity and Retention:

Remote logging (all systems sending their log records to a centralized log server that is locked down against attack and data modification) provides protection from post-incident log file cleansing.

There’s no single solution. Get familiar with your system.

Reporting and Documenting Investigations: part of organization’s policy and procedures

Preparing formal documentation lays the foundation for escalation and potential legal action

Organizations should ensure that anyone involed in the collection or analysis of potential evidence receive proper training

It’s a good idea to establish a relationship with your corporate legal personnel and the appropriate law enforcement agencies. In advance, identify a single point of contact in your organization who will act as your liaison with law enforcement. It benefits 2 things:

Law enforcement hears a single perspective from your organization and knows the “go-to” person for updates

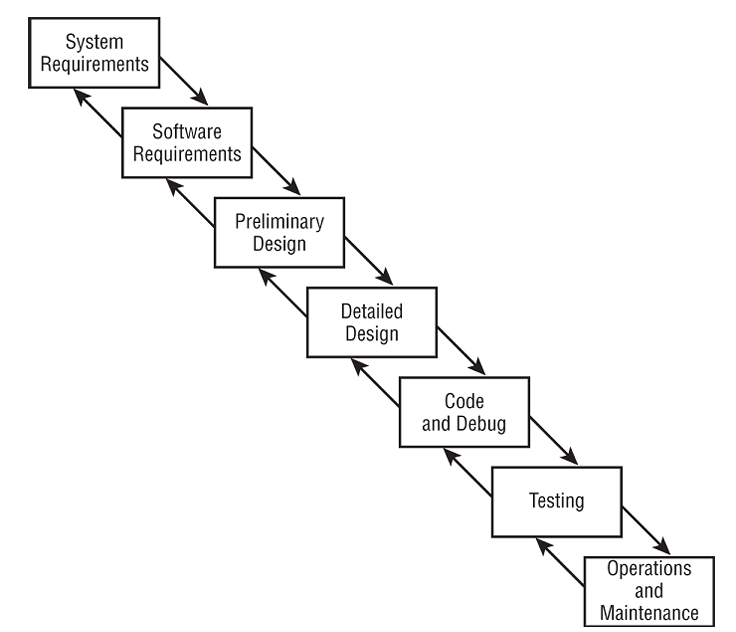
Allows the predesignated contact to develop working relationships with law enforcement personnel

Optional: participate in the FBI’s InfraGard program (infragard.org)

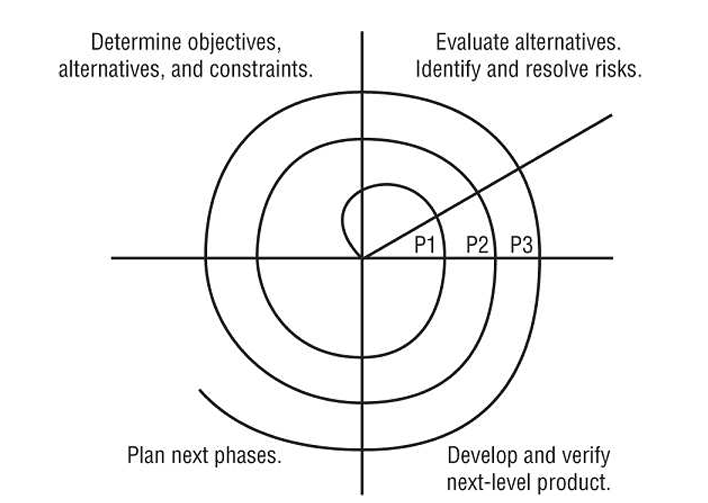
1. Major Categories of Computer Crime (mostly focusing on their goals)
   1. Military and intelligence attacks:
      1. Military descriptive infromation of any type, including deployment information, readiness information, and order of battle plans
      2. Secret intelligence gathered for military or law enforcement purposes
      3. Descriptions and storage locations of evidence obtained in a criminal investigation
      4. Any secret information that could be used in a later attack
   2. Business attacks: Focus on illegally jeopardizing the CIA of information and systems operated by a business. Corporate espionage has become a big threat. Trade secrets are vulnerable. Information gathered during the attack usually causes more damage than the attack itself.
   3. Financial attacks: shoplifting, burglary, DDoS, cybercrime for hire (engaging in mercenary activity) . Credit card numbers and fraudulent funds transfers are their goals.
   4. Terrorist attacks: Possible targets are power plants, telecommunications, power distribution.
   5. Grudge attacks: Possible targets are current or former employee
      1. The insider threat: as soon as an employee is terminated, all system access for that employee should be terminate to reduces the likelihood of this type of threat. However, diligent monitoring and assessing systems for vulnerabilities is the best protection from most grudge attacks.
   6. Thrill attacks: The main motivation is the “high” of successfully breaking into a system. The common one involves website defacements (replacing an organization’s legitimate web content with other pages to boast their attacks’ skills).
   7. Hacktivist (combination of hacker and activist) attacks: often combine political motivations with the thrill of hacking. Their purpose is to disrupt the activity of organizations that they differ with philosophically though they feel that they have nothing to lose and don’t hide their activity. They usually loosely group together with names. DoS attack is common due to little knowledge required.

Domain 8: Software Development Security

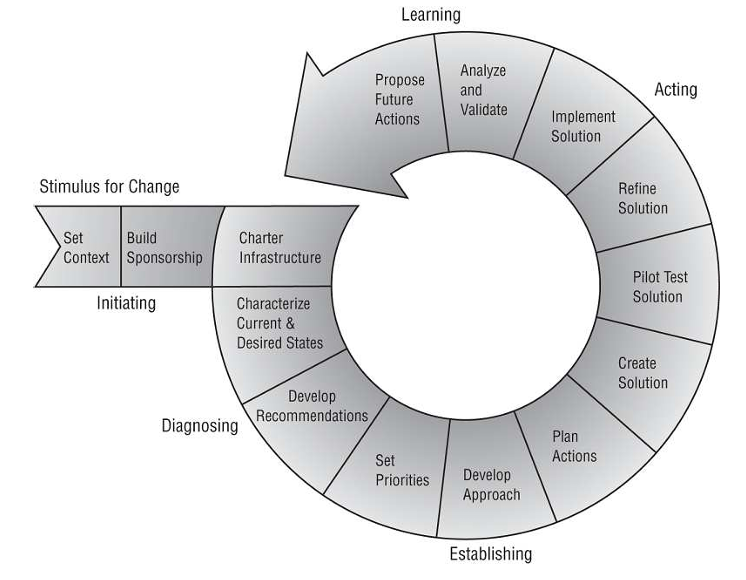
1. Introducing Systems Development Controls (Chapter 20)
   1. Software Development
      1. Programming Language: You’ll learn more about the exploit attackers use to undermine software in the section “Application Attacks” in Chapter 21, “Malicious Code and Application Attacks”.
      2. Libraries: Over the years, the use of shared libraries has resulted in many security issues. One of the most well-known and damaging examples of this is the Heartbleed vulnerability (CVE-2014-0160) that struck the OpenSSL library in 2014.
      3. Development Toolsets: Just talk about IDEs
      4. Object-Oriented Programming: some common OOP terms you might come across in your work:
         1. Message: input of an object
         2. Method: the internal functions
         3. Behavior: output of the methods given the input
         4. Class
         5. Instance
         6. Inheritance
         7. Delegation: let the other object define the functions
         8. Polymorphism: external conditions that change the output of the same method with same input
         9. Cohesion: like isomorphism in abstract algebra where the functions are methods
         10. Coupling: level of interaction between objects. Lower coupling provides better software design because objects are more independent.
      5. Assurance: The Common Criteria provide a standardized approach to assurance used in government settings. For more information on assurance and the Common Criteria, see Chapter 8, “Principles of Security Models, Design, and Capabilities.”
      6. Avoiding and Mitigating System Failure:
         1. Input Validation: limit check, escaping input
         2. Authentication and Session Management
         3. Error Handling: Developers should disable detailed error messages (known as debugging mode) on any servers and applications that are publicly accessible.
         4. Logging: The OWASP Secure Coding Practices suggest logging the following events:
            1. Input validation failures
            2. Authentication attempts, especially failures
            3. Access control failures
            4. Tampering attempts
            5. Use of invalid or expired session tokens
            6. Exceptions raised by the operating system or applications
            7. Use of administrative privileges
            8. TLS failures
            9. Cryptographic errors (can be useful in diagnosing security issues and in the investigation of security incidents)
         5. Fail-Secure and Fail-Open: Blue Scree of Death (BSOD) is an example of fail-secure.
   2. Systems Development Lifecycle:
      1. Conceptual Definition: The conceptual definition is a very high-level statement of purpose and should not be longer than one or two paragraphs. The security requirements developed at this phase are generally very high level and will be refined in the **control specifications development** process.
      2. Functional requirements determination: specific system functionalities are listed, and developers begin to think about how the parts of the system should interoperate to meet the functional requirements: input(s), behavior, and output(s).
      3. Control specifications development: you should analyze the system from a number of security perspectives:
         1. Adequate access controls must be designed into every system to ensure that only authorized users are allowed to access the system.
         2. The system must maintain the confidentiality of vital data through the use of appropriate encryption and data protection technologies.
         3. The system should provide both an audit trail to enforce individual accountability and a detective mechanism for illegitimate activity.
         4. Depending on the criticality of the system, availability and fault-tolerance issues should be addressed as corrective actions.
      4. Design review: the designers determine exactly how the various parts of the system will interoperate, how the modular system structure will be laid out, and (commonly) sets specific tasks for various teams and lays out initial **timelines** for the completion of coding **milestone**s.
      5. Coding: Developers should use the **security software coding principles** discussed in this chapter to craft code that is consistent with the agreed-upon design and meets user requirements.
      6. Code review walk-through: project managers should schedule several code review walk-through meetings at various milestones throughout the coding process.
      7. System test review: Once developers are satisfied that the code works properly, the process moves into user acceptance testing (UAT), where users verify that the code meets their requirements and formally accept it as ready to move into production use.
      8. Maintenance and change management
   3. Lifecycle Models: Barry Boehm proposed several software development lifecycle (SDLC) models:
      1. Waterfall Model: the waterfall model focuses on a large-scale effort to deliver a finished system

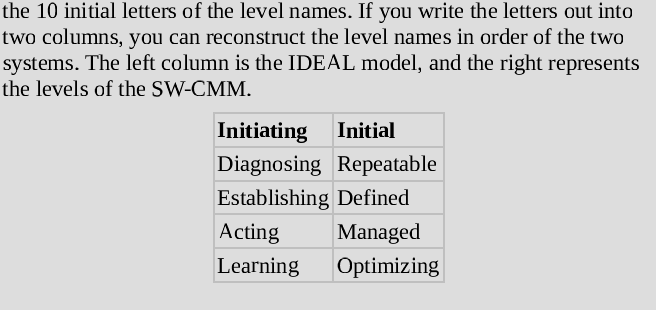


* + 1. Spiral Model: focuses on iterating through a series of increasingly “finished” prototypes that allow for enhanced quality control. It provides a solution to the major criticism of the waterfall model-it allows developers to return to the planning stages as changing technical demands and customer requirements necessitate the evolution of a system.

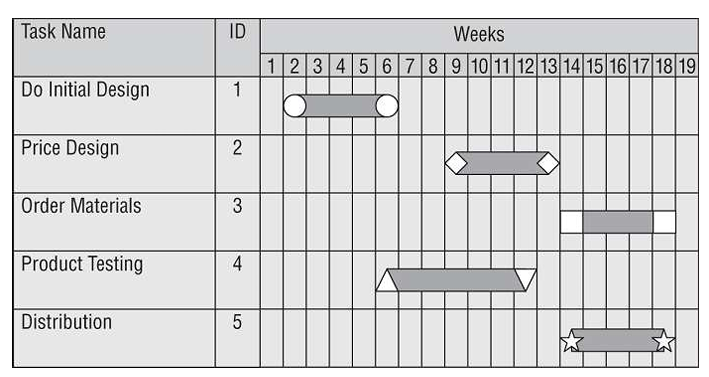


* + 1. Agile Software Development: 17 pioneers of the Agile development approach got together in 2001 and produced a document titled Manifesto for Agile Development (agilemanifesto.org) that states the core philosophy of the Agile approach:
       1. Through this work we have come to value:
          1. **Individuals and interactions** over processes and tools
          2. **Working software** over comprehensive documentation
          3. **Customer collaboration** over contract negotiation
          4. **Responding to change** over following a plan
       2. 12 principles that underlie the philosophy, which are available here:
          1. Our highest priority is to satisfy the customer through early and continuous delivery of valuable software
          2. Welcome changing requirements, even late in development. Agile processes harness change for the customer’s competitive advantage.
          3. Deliver working software frequently, from a couple of weeks to a couple of months, with a preference to the shorter timescale.
          4. Business people and developers must work together daily throughout the project
          5. Build projects around motivated individuals. Give them the environment and support they need, and trust them to get the job done.
          6. The most efficient and effective method of conveying information to and within a development team is face-to-face conversation.
          7. Working software is the primary measure of progress.
          8. Agile processes promote sustainable development. The sponsors, developers, and users should be able to maintain a constant pace indefinitely.
          9. Continuous attention to technical excellence and good design enhances agility.
          10. Simplicity-the art of maximizing the amount of work not done-is essential
          11. The best architectures, requirements, and designs emerge from self-organizing teams.
          12. At regular intervals, the team reflects on how to become more effective, then tunes and adjusts its behavior accordingly.
    2. Capability Maturity Model (CMM, SW-CMM, or SCMM): the stages of the SW-CMM are as follows:
       1. Initial: you’ll often find hardworking people charging ahead in a disorganized fashion. There’s usually little or no defined software development process.
       2. Repeatable: basic lifecycle management processes are introduced.
       3. Defined: software developers operate according to a set of formal, documented software development processes.
       4. Managed: Quantitative measures are used to gain a detailed understanding of the development process
       5. Optimizing: Sophisticated software development processes are in place that ensure that feedback from one phase reaches to the previous phase to improve future results.
    3. Software Assurance Maturity Model (SAMM)
       1. Governance: includes practices for strategy, metrics, policy, compliance, education, and guidance
       2. Design: include practices for threat modeling, threat assessment, security requirements, and security architecture.
       3. Implementation: includes the secure build, secure deployment, and defect management practices
       4. Verification: includes architecture assessment, requirements-driven testing, and security testing.
       5. Operations: includes incident management, environment management, and operational management.
    4. IDEAL Model
       1. Initiating: outlines the business reasons behind the change, build support for the initiative, put in place the appropriate infrastructure
       2. Diagnosing: engineers analyze the current state of the organization and make general recommendations
       3. Establishing: the organization takes the general recommendations from the diagnosing phase and develops a specific plan of action that helps achieve those changes.
       4. Acting: develops solutions and tests, refines, and implements them.
       5. Learning: continuously analyze its efforts to determine whether it has achieved the desired goals, and when necessary, propose new actions to put the organization back on course.

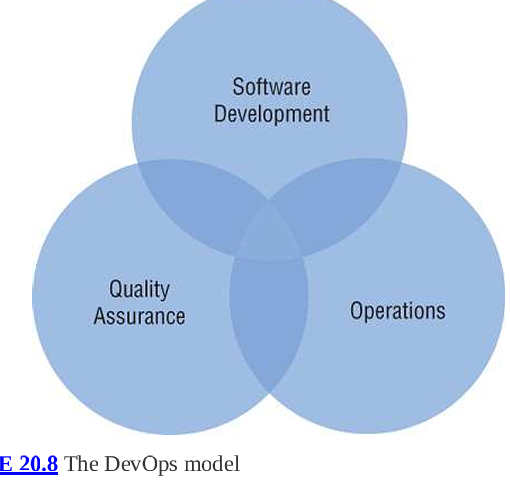




* + 1. Gantt Charts and PERT:
       1. A Gantt chart is a type of bar chart that shows the interrelationships over time between projects and schedules



* + - 1. PERT (program evaluation review technique): a project-scheduling tool used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment.
  1. Change and Configuration Management
     1. The change management has 3 basic components:
        1. Request Control: users can request modifications, managers can conduct cost/benefit analysis, and developers can prioritize tasks
        2. Change Control: developers re-create the situation encountered by the user and to analyze the appropriate changes to remedy the situation.
        3. Release Control: double-check and ensure that any code inserted as a programming aid during the change process (like debugging code and/or backdoors) is removed before releasing the new software to production. Release control should also include acceptance testing to ensure that any alterations to end-user work tasks are understood and functional.
     2. Software configuration management (SCM): 4 main components:
        1. Configuration Identification: administrators document the configuration of covered software products throughout the organization
        2. Configuration Control: updates can be made only from authorized distributions in accordance with those policies
        3. Configuration Status Accounting: formalized procedures are used to keep track of all authorized changes that take place
        4. Configuration Audit: ensure the actual production environment is consistent with the accounting records and no unauthorized configuration changes have taken place.
  2. The DevOps Approach: The DevOps seeks to resolve the issues by bringing the three functions together in a single operational model. The DevOps is closely aligned with the Agile development approach. Some organizations even strive to reach the goal of continuous integration/continuous delivery (CI/CD), where code may roll out dozens or even hundreds of times per day.



* 1. Application Programming Interfaces:

A social media API might include some of the following API function calls:

* + - 1. Post status
      2. Follow user
      3. Unfollow user
      4. Like/Favorite a post
  1. Software Testing: You should not use live or actual field data for testing, especially in the early development stages.
     1. Reasonable check: ensures that values returned by software match specified criteria that are within reasonable bounds.
     2. Use cases: mirror normal activity
     3. Misuse cases: attempt to model the activity of an attacker
     4. White-Box Testing
     5. Black- White- Gray-Box Testing
  2. Code Repositories: provide several important functions supporting these collaborations (like GitHub, Bitbucket, and SourceForge).
  3. Service-Level Agreement (SLAs): common issues are addressed in SLAs:
     1. System uptime (as a percentage of overall operating time)
     2. Maximum consecutive downtime (in seconds/minutes/and so on)
     3. Peak load
     4. Average load
     5. Responsibility for diagnostics
     6. Failover time (if redundancy is in place)
  4. Third-Party Software Acquisition:
     1. Commercial off-the-shelf (COTS) software: run on servers managed by the organization, either on premises or in an IaaS enviroment. Other software is purchased and delivered over the internet through web browsers, in a SaaS approach.
     2. Community-based open source software (OSS) projects

1. Storage Threats: Chapter 9, “Security Vulnerabilities, Threats, and Countermeasures,” included a comprehensive look at different types of storage.
   1. The threat of illegitimate access to storage resources exists no matter what type of storage is in use.
   2. Covert channel attacks
2. Understanding Knowledge-Based Systems:
   1. Expert Systems: are not infallible-they’re only as good as the data in the knowledge base and the decision-making algorithms implemented in the inference engine. However, they have one major advantage in stressful situations-their decisions do not involve judgement clouded by emotion. They might contain the following statements (example only)
      1. If the hurricane is a Category 4 storm or higher, the flood waters normally reach a height of 20 feet above sea level.
      2. If the hurricane has winds in excess of 120 miles per hour (mph), then wood-frame structures will be destroyed.
      3. If it’s late in the hurricane season, then hurricanes tend to get stronger as they approach the coast.
   2. Machine Learning:
      1. Supervised learning techniques: use labeled data for training
      2. Unsupervised learning techniques: use unlabeled data for training
   3. Neural Networks: an extension of machine learning techniques.
3. Malware (Chapter 21)
   1. Sources of Malicious Code: scripts downloaded from the internet. International organized crime syndicates are known to play a role in malware proliferation. The most recent trend in malware development comes with the rise of the advanced persistent threat (APT). APTs are sophisticated adversaries with advanced technical skills and significant financial resources.
   2. Virus: it’s payload delivers whatever malicious activity the virus writer had in mind.
   3. Virus Propagation Techniques
      1. Master Boot Record (MDR) Viruses: attack the MBR-the portion of bootable media (like hard disk or flash drive) that the computer uses to load the operating system during the boot process.
      2. File Infector Viruses: slightly alter or replace entirely the code of executable files. Its variation is the **companion virus:** self-contained executable files that escape detection by using a filename similar to, but slightly different from, a legitimate operating system file. For example, if you had a program on your hard disk named game.exe, a companion virus might use the name game.com. If you then open a command prompt and simply type GAME, the operating system would execute the virus file, game.com, instead of the file you actually intended to execute.
      3. Macro Viruses: basically like macros (used for repetitive tasks) but malicious.
      4. Service Injection Viruses: infect systems and escape detection-injecting themselves in to trusted runtime processes of the operating system, such as svchost.exe, winlogon.exe, and explorer.exe.
   4. Virus Technologies
      1. Multipartite Viruses: use more than one propagation technique
      2. Stealth Viruses: hide themselves by actually tampering with the operating system to fool antivirus packages into thinking that everything is functioning normally.
      3. Polymorphic Viruses: modify their own code as they travel from system to system. However, antivirus vendors have “cracked the code” of many polymorphism techniques, so current versions of antivirus software are able to detect known polymorphic viruses.
      4. Encrypted Viruses: They use a very short segment of code (virus decryption routine) containing the cryptographic information necessary to load and decrypt the main virus code stored elsewhere on the disk. Each infection utilizes a different cryptographic key, causing the main code to appear completely different on each system.
   5. Hoaxes: www.snopes.com/tag/virus-hoaxes-realities
   6. Logic Bombs
   7. Trojan Horses
   8. Botnets
   9. Worms
      1. Code Red Worm:
         1. Randomly selected hundreds of IP addresses and then probed those addresses to see whether they were used by hosts running a vulnerable version of IIS. Any systems it found were quickly compromised. This greatly magnified Code Red’s reach because each host it infected sought many new targets.
         2. It defaced HTML pages on the local web server, replacing normal content with the following text:

Welcome to <http://www.worm.com!>

Hack By Chinese!

* + - 1. It plainted a logic bomb that would initiate a DoS attack against the IP address 198.137.240.91, which at that time belonged to the web server hosting the White House’s home page. Quick-thinking government web administrators changed the White House’s IP address before the attack actually began.
    1. RTM and the Internet Worm: This worm spread by exploiting four specific security holes in the Unix operating system:
       1. Sendmail Debug Mode
       2. Password Attack
       3. Finger Vulnerability
       4. Trust Relationships
    2. Stuxnet:
       1. Searching for unprotected administrative shares of systems on the local network
       2. Exploiting zero-day vulnerabilities in the Windows Server service and Windows Print Spooler service
       3. Connecting to systems using a default database password
       4. Spreading by the use of shared infected USB drives
  1. Spyware and Adware: Spyware monitors your actions and transmits important details. Adware has different purpose: displaying advertisements. Both of them fit into a category of software known as potentially unwanted programs (PUPs), software that a user might consent to installing on their system that then carries out functions that the user did not desire or authorize.
  2. Ransomware: weaponizes cryptography. Paying ransom for the purpose of recovering data may be illegal.
  3. Malicious scripts: usually written in PowerShell, Bash…
  4. Zero-Day Attacks: 2 main reasons systems are affected by this:
     1. The necessary delay between the discovery of a new type of malicious code and the issuance of patches and antivirus updates (**window of vulnerability**).
     2. Slowness in applying updates on the part of system administrators.

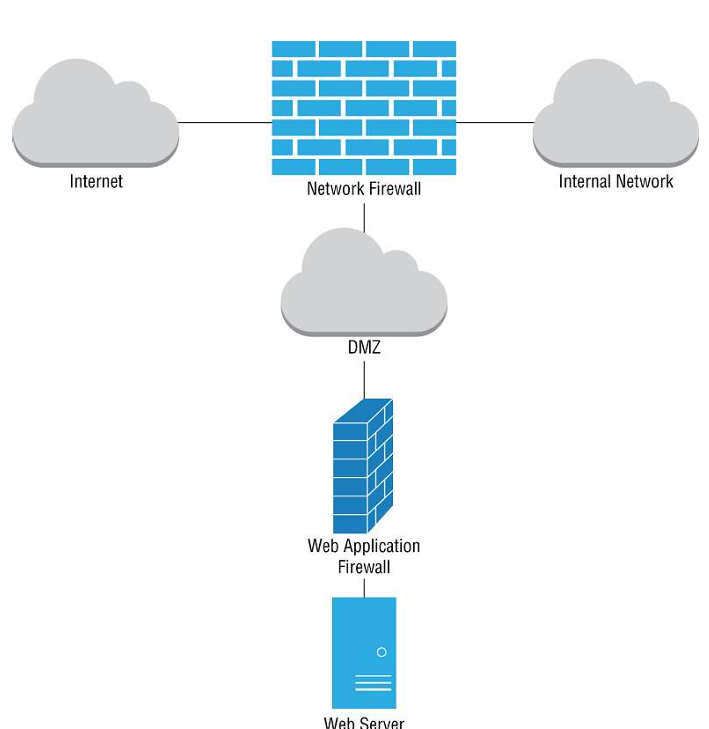
1. Malware Prevention
   1. Platforms Vulnerable to Malware: researchers estimated in a 2020 analysis by av-test.org that 83% of malware in existence targets the Windows platform.
   2. Antimalware Software: performs one of the following actions if it detects malware:
      1. If the software can eradicate the virus, it disinfects the affected files and restores the machine to a safe condition.
      2. If the software recognizes the virus but doesn’t know how to disinfect the files, it may quarantine the files until the user or an administrator can examine them manually.
      3. If security settings/policies do not provide for quarantine or the files exceed a predefined danger threshold, the antivirus package may delete the infected files in an attempt to preserve system integrity.

Heuristic mechanisms: analyze the behavior of software, look for the telltale signs of virus activity, cover their electronic tracks, and alter unrelated or operating system files.

A common strategy is for systems to quarantine suspicious files and send them to a malware analysis tool (executed in an isolated but monitored environment).

* 1. Integrity Monitoring: alert administrators to unauthorized file modifications, detect web server defacements and similar attacks, provide some warning of virus infections if critical system executable files.
  2. Advaced Threat Protection
     1. Endpoint detection and response (EDR):
        1. Analyzing endpoint memory, filesystem, and network activity for signs of malicious activity
        2. Automatically isolating possible malicious activity to contain the potential damage
        3. Integration with threat intelligence sources to obtain real-time insight into malicious behavior elsewhere on the internet
        4. Integration with other incident response mechanisms to automate response efforts.

1. Application Attacks
   1. Buffer Overflows
   2. Time of Check (TOC) to Time of Use (TOU): Attackers can develop attacks based on the predictability of task execution. TOC is the time at which the subject checks on the status of the object. When the decision is made to access the object, the procedure accesses it at the TOU. TOC/TOU attacks are oftenn called race conditions because the attacker is racing with the legitimate process to replace the object before it’s used.
   3. Backdoors: undocumented command sequences that allow individuals with knowledge of the backdoor to bypass normal access restrictions. Usually used by developers to debug and then forgotten.
   4. Privilege Escalation and Rootkits
2. Injection Vulnerabilities
   1. SQL injection Attacks
   2. Blind Content-Based SQL Injection: tests whether the application is interpreting injected code before attempting to carry out an attack.
   3. Blind Timing-Based SQL Injection: use the amount of time required to process a query as a channel for retrieving information from a database
   4. Code Injection Attacks: SQL injection, XML injection, LDAP injection, CSRF
   5. Command Injection Attacks
3. Exploiting Authorization Vulnerabilities
   1. Insecure Direct Object References: like using URL to get the items
   2. Directory Traversal
   3. File Inclusion
      1. Local file inclusion attacks: seek to execute code stored in a file located elsewhere on the web server.
      2. Remote file inclusion: attackers can directly control the code being executed without having to first store a file on the local server
4. Exploiting Web Application Vulnerabilities
   1. XSS
      1. Reflected XSS
      2. Stored/Persistent XSS
      3. Request Forgery
      4. CSRF/XSRF
      5. Server-Side Request Forgery (SSRF): trick a server into visiting a URL based on user-supplied input
   2. Session Hijacking
5. Application Security Controls
   1. Input Validation
   2. Web Application Firewalls (WAFs): function similarly to network firewalls, but they work at the Application layer of the OSI model



* 1. Database Security
     1. Parameterized Queries and Stored Procedures: the developers prepares a SQL statement and then allows user input to be passed into that statement as carefully defined variables that do not allow the insertion of code. Java uses the PreparedStatement() function while PHP uses the bindParam() function. Stored procedures doesn’t not contain the SQL code within the application but store it on the database server and the client sends argument to the server instead.
     2. Obfuscation and Camouflage:
        1. Data minimization
        2. Tokenization
        3. Hashing
  2. Code Security
     1. Code signing (digitally): confirm the authenticity of developers’ code to the end users
     2. Code Reuse: making a third-party software libraries and software development kits (SDKs) for reuse
     3. Software Diversity: to avoid single points of failure
     4. Code Repositories: centralized locations for the storage and management of application source code, for secure storage, for the coordination of changes among multiple developers, for performing version control, for code reuse, and for avoiding the problem of dead code (where nobody is responsible for the maintenance)
     5. Integrity Measurement
     6. Application Resilience
        1. Scalability: applications should be designed so that computing resources they require may be incrementally added to support increasing demand
        2. Elasticity: applications should be able to automatically deprovision those resources to reduce capacity (and cost) when they’re not longer needed
  3. Secure Coding Practices
     1. Source Code Comments: good for workflow but may provide attackers with a road map explaining how code works.
     2. Error Handling
     3. Hard-Coded Credentials
        1. 1st version: developer may create a hard-code maintenance account for the application that allows developer to regain access even if the authentication system fails (known as backdoor vulnerability)
        2. 2nd version: developers include access credentials for other services within their source code
     4. Memory Management
        1. Resource Exhaustion: memory leaks are an example of resource exhaustion. If an application requests memory from the operating system, it will eventually no longer need that memory and should then return the memory to the operating system for other uses.
        2. Pointer Dereferencing